REQUEST FOR PROPOSAL

FOR

Implementation of a Comprehensive Log Management, Event Correlation, Database Activity Monitoring & Vulnerability Management Solutions

TECHNOLOGY MANAGEMENT DEPARTMENT
HEAD OFFICE, 66, RAJAJI SALAI,
CHENNAI – 600 001

Website: www.indianbank.in

INDEX

SECTION -1

Activity Schedule

The schedule is subject to change and notice in writing of any changes will be provided wherever feasible.

Sl No	Activity	Details
1.	**RFP/Bid date**	05.09.2012
2.	**Bid document Price : (non-refundable)**	INR.10,000/-. The amount has to be paid by way of a Demand Draft (DD) favoring INDIAN BANK payable at CHENNAI and to be enclosed along with Part I of bid documents.
3.	**Address for submission of Bid**	Assistant General Manager Indian Bank, Corporate Office**,** Expenditure Department 254-260, Avvai Shanmugham Salai, Royapettah, Chennai 600 014, India
4	**Bid submission**	Bid forms can be downloaded from our website www.indianbank.in Bid to be submitted : 1. Part-I :- Technical The envelope containing the Part-I bids should be placed along with the DD towards Bid Document price with the superscription "**Implementation of a Comprehensive Log Management, Event Correlation, Database Activity Monitoring & Vulnerability Management Solutions**"
5.	**Last date for Submission of Bid**	**27.09.2012– 1600 Hours**
6.	**BID SECURITY (EARNEST MONEY DEPOSIT)**	Rs.10,00,000/- in the form of Bank Guarantee in favour of INDIAN BANK issued by a scheduled bank and valid for sixty (60) days beyond the validity of the bid and to be enclosed along with bid Part I documents.
7.	**Bid opening date / time / venue**	Part-I : - The bids will be opened on 27.09.2012 at about 16.30 Hours at the address mentioned in SL No:3. Part- II: - Technically qualified bidders of Part I will be informed the date of reverse auction at a later date.
8.	**a) Pre Bid Meeting** **b) Contact details :**	12.09.2012 at 11.30 a.m in the following address: Assistant General Manager(TMD) INDIAN BANK, **Head Office** Technology Management Department, 66, Rajaji Salai, Chennai 600 001 Ph: 91-44-25260112, 25250155 email: asif.sa@indianbank.co.in; issc@indianbank.co.in
9.	**Language of the Bid**	This bid should be filled in English language only. If any supporting documents submitted are in any language other than English, translation of the same in English language is to be duly attested by the bidder.
10.	**Official website**	**www.indianbank.in**

IMPORTANT NOTICE

- **This tender document is not transferable.**

- Bidders are advised to study the tender document carefully. Submission of bid shall be deemed to have been done after careful study and examination of the tender document with full understanding of its implications.

- The response to this tender should be full and complete in all respects. Incomplete or partial bids will be liable for rejection. The bidder must quote for all the items.

- The bidder shall bear all costs associated with the preparation and submission of the bid, including cost of presentation for the purposes of clarification of the bid, if so desired by the bank. The bank will in no case be responsible or liable for those costs, regardless of the conduct or outcome of the bidding process.

- The bank reserves the right to reject the bidder's assertion of compliance to a requirement, if the detailed response is found unsatisfactory or contradictory.

- The bank may extend the time for submission of all the proposals.

- Bank reserves the right to negotiate with successful bidder under exceptional circumstances.

- Bank has right to cancel the tender on its discretion without assigning any reason therefor.

- Part II of the BID will be through online reverse auction process. Technically eligible bidders will be informed to participate in the online reverse auction process. The authorised official of the bidders should have digital certificate to participate in the online reverse auction process.

- Bidders are requested to view our website www.indianbank.in for the modifications/updations/clarification made by the Bank, if any, as related communications will be made available only in the website.

SECTION -2

INTRODUCTION

2. INTRODUCTION

Indian Bank, a leading Public Sector Bank having its Head Office at Chennai has national presence in more than 1956 locations spreading over 33 Zones and international presence in Singapore and Sri Lanka. It has been serving the nation with a team of dedicated staff for more than 100 years. As on 30.06.2012, the Bank's business reached Rs.2,20,888 crores.

The Bank is engaged in diversified banking activities. The Bank is a pioneer in introducing the latest technology in Banking having implemented Core Banking Solution in all the branches covering 100% of Business. Internet Banking services are available to all the customers. The Bank has also implemented other delivery channels like Mobile/Phone Banking, ATM & provides variety of e-payment channels for its customers.

2. 1. INDIAN BANK's I T INFRASTRUCTURE

A. DATA CENTRE (DC)/ DISASTER RECOVERY SITE (DR)

Bank has its Data Centre at Chennai and Disaster Recovery Site at Hyderabad with link level and device level redundancies

B. ENTERPRISE WIDE NETWORK:

The Bank has established a Wide Area Network covering all offices and core banking branches. Connectivity for Core Banking at branches is at present through MPLS to the Central Data Centre at Chennai. The branch level connectivity is through VSAT or leased lines with ISDN/VSAT/GPRS backup. Delivery channels like ATMs (Onsite & Offsite), Internet, Mobile, Phone Banking, RTGS, NEFT also form part of the network.

C. SECURITY INFRASTRUCTURE

Bank has a well-established Security Operations Center (SOC) at Chennai operating on a 24 x 7 basis. The SOC activities include security devices monitoring and management viz firewall, NIPS and HIDS, asset & patch management, vulnerability assessment, anti-phishing services, incident management & resolution, anti-virus management etc.

SECTION 3

INVITATION FOR BIDS (IFB)

3. INVITATION FOR BIDS (IFB)

3.1 Indian Bank invites sealed quotations from all eligible bidders for **Implementation of a Comprehensive Log Management, Event Correlation, Database Activity Monitoring & Vulnerability Management Solutions**.

3.2 The cost of the bid document is Rs.10,000/-. The amount has to be paid by way of a Demand Draft (DD) favouring INDIAN BANK payable at CHENNAI. The bidders can download the bid document from our Website. Bidders have to submit a DD for Rs.10,000/- towards the cost of bid document along with Part I - the technical bid in a separate cover. Bid documents without this fee is liable for rejection.

3.3 Further information can be had from the bank at the address given below from 10.00 to 17.00 hours on all days from Monday to Friday and from 10.00 to 14.00 hours on Saturdays, except Bank holidays:

Assistant General Manager (TMD/ ISSC)
INDIAN BANK,
Head Office,
Technology Management Department
66, Rajaji Salai
Chennai 600 001
Phone No:91-44-25260112
Email: asif.sa@indianbank.co.in; issc@indianbank.co.in

3.4 Bids must be delivered to the address given below, on or before 16.00 hours IST on 27.09.2012 and must be accompanied by a Bank Guarantee (Bid Security) of Rs.10,00,000/-.

Assistant General Manager
Indian Bank,Corporate Office,
Expenditure Department
254-260, Avvai Shanmugham Salai,
Royapettah, Chennai 600 014, India
Ph: 28134300

Late Bids will not be accepted. The bid consist of one part viz., Part I – Technical Bid. Part II – Commercial bid will be through online reverse auction process.

3.5 Part I (technical bid) will be opened for evaluation by the Bank at 16.30 Hours on 27.09.2012 in the presence of the bidders or their authorised representatives. Bidders are requested to be present on this date and time at the above address as mentioned in 3.4.

After technical evaluation, only the eligible bidders will be communicated of the date and time for reverse auction.

SECTION 4

DESCRIPTION AND SCOPE OF THE ASSIGNMENT

4. DESCRIPTION AND SCOPE OF THE ASSIGNMENT

4.1 The name of the assignment is '**Implementation of a Comprehensive Log Management, Event Correlation , Database Activity Monitoring Solutions and Vulnerability Management Solutions**'.

4.2 The brief description of the Assignment are

Deployment of a comprehensive log management and event correlation solution using a combination of Log Management, EVENT CORRELATION, Database Activity Monitoring, Vulnerability Management solutions that will monitor the entire IT infrastructure (LAN, WAN, Business & all supporting applications and databases) of the Bank spread over Data Centre, DR Site, Corporate Office, Head Office, Zonal Offices and Branches located all over India. Security Incident and Event Monitoring must be an enterprise solution for aggregating, correlating and analysing security event data in real time. The solution must help the bank to identify and promptly respond to threats, demonstrate compliance with regulatory requirements, and perform the required forensic activities.
The Centralised Log And Event Correlation solution shall collect and centrally store all log data, manage event log data and provide full functions, real time event monitoring and management capabilities. The solution must provide the Bank with significant capabilities to collect, correlate analyse, detect and proactively respond to security threats originating from both inside and outside the Bank.

The Database Activity Monitoring (DAM) Solution shall have the ability to independently monitor and audit all databases activities, administrator activities and all DML transactions including SELECT commands.
The Vulnerability Management Solution must be capable of monitoring the IT assets' and identifying the vulnerabilities associated with them along with the location of such vulnerability and suggest the mitigation steps.

4.3 The Bank intends to implement the above towards its objectives to strengthen the security infrastructure and ensure the availability of resources to authorised users without any disruption or degradation.

4.4 The deployment will be at Chennai and Hyderabad. The Bank reserves the right for change in location, in case of need.

4.5 The bidder should provide one onsite personnel support during office hours (9:00 AM to 6:00 PM) on all working days and offsite support during non-business hours. At times of exigencies during non-business hours, onsite support must be made available within 3 hours from the time of call for support without any additional cost.

4.6 Solution Requirements

The solution should be able to collect logs at present from 4 sites (3 sites at Chennai and 1 at Hyderabad).
The Bank has DC at Chennai and DR at Hyderabad.
The devices/appliances proposed for the solution at DC & DR must be

- Identical
- Rack mountable with necessary perforated racks (front & back) and rails.
- Must be in active-passive mode with High Availability(HA) /Failover features wherever required in the solution.
- Having hot swappable dual power supply
- Solution must comply all the **Technical Specifications** mentioned under **Section 8** and as per **section 9.8**.
- Under Section 8: In case of customizable, Maximum 2 line items under each Major heading can be permissible for customization in terms of features and not hardware. The customization also should be finished within stipulated timeline of implementation of project as mentioned in RFP. **In case if any feature is not readily available & also non customizable, the bid will be liable for rejection.**
- Entire proposed solutions should have unlimited user licenses wherever applicable.

4.7 The Scope of Work

4.7.1 Centralized Log Management and Event Correlation

i. Log Collection

Logs from all the in-scope devices located at the geographically dispersed locations should be collected. The successful Bidder should develop the baseline for the level of logs to be enabled from different components of IT infrastructure assets. The log baseline should be in line with global best practices. In case the systems/applications are writing logs to the local hard disks, solution should be capable to pull the logs from these devices through secure transfer. Only in case where remote log collection is not feasible, the successful bidder should install agent on the servers and applications for collection of logs. Raw logs should be made available in case of legal requirement.

ii. Log Aggregation and Normalization

Logs collected from all the devices should be aggregated as per the user configured parameters. Logs from multiple disparate sources should be normalized in a common format for event analysis and correlation.

iii. Log Encryption, Compression and Transmission

Collected logs should be encrypted and compressed before the transmission to the remote Log Correlation Engine.

iv. Log Archival

Raw Logs collected from all the devices should be stored in a non-tamperable format as defined in the technical specifications for log storage. Collection of Logs and storage should comply with the Regulatory requirements and should maintain a chain of custody to provide the same in the court of law, in case the need arises. For correlation and report generation purpose, at least past 1 year log data should be available online.

Solution being provided should be scalable and user configurable to cater to the future requirements of the Bank.

Retrieval of archived logs should not require any proprietary tools/protocol and should be retrievable using open standards/protocols or else the retrieval tool should be provided to the Bank at no extra cost.

v. Log Correlation

Collected Logs should be correlated according to various predefined criteria for generation of alert and identification of the incident. The correlation rules should be predefined and also user configurable. Correlation rules should be customized by bidder on regular basis to reduce false positives. In any case False negatives will not be permitted. In case of detection of any such incident, correlation rules must be customized immediately to capture such incidents. The correlation activity must be through a systematic process of correlating event data to identify attacks and frauds. It must have proper analysis and reporting tools for investigation and compliance purposes. The output of correlated logs should be stored in system for future reference.

vi. Alert Generation

Solution should be capable to generate alerts, register and send the same through message formats like SMTP, SMS, SNMP etc. as per user configurable parameters.

vii. Event Viewer/Dashboard/Reports/Incident Management

Centralised Log And Event Correlation Solution should provide web based facility(multi user concurrent sessions) to view security events and security posture of the Bank's Network and register incidents. Solution should have drill down capability to view deep inside the attack and analyze the attack pattern. Dash board should have filtering capability to view events based on various criteria like geographical location, Device type, attack type etc. Dashboard should have Role based (e.g. Application team/Network team/security team/Database team etc.) as well as Discretionary access control facility to restrict access to incidents based on user security clearance level. Solution should provide various reports based on user configurable parameters and standard compliance reports like PCI-DSS, ISO27001, IT Act and regulatory reports.

Successful bidder will customize incident management/dashboard/reports for the Bank and will modify the same as per the changing requirement of the Bank.

4.7.2 Database Activity Monitoring

Solution should provide Database activity monitoring capability for all the DBA and maintenance related access as well as transaction related access by various applications including SQL queries. DAM tool has to be integrated with the Centralised Log And Event Correlation tool, Incident Management tool. Tool shall record all SQL transactions: DML, DDL, and DCL Activity. It must store this activity securely outside the database. It must aggregate and correlate activity from multiple heterogeneous Database Management Systems (DBMSs). It must enforce separation of duties on database administrators. It must generate alerts on policy violations.

4.7.3 Vulnerability Management Tool

The solution should be capable to monitor the infrastructure assets' vulnerabilities along with the location of such vulnerability and suggest the mitigation steps. Vulnerability scanning has to be performed on a periodic basis. VM tool has to be integrated with the Centralised Log And Event Correlation solution, Incident

Management and Security dashboard.

Successful bidder should assess the Bank's environment against the baseline on periodic basis and ensure that Baseline is maintained on an ongoing basis.

4.7.4 Integration with Incident Management tool

Solution should be able to integrate with different tools such as Log Management And Event Correlation tool, Database Activity Monitoring tool, Vulnerability Management tool etc. Incident management should include escalation as per the escalation matrix. Solution should be able to send the incident report in various forms like e-mail, SMS etc.

Bank has Adventnet Trouble Ticketing Tool and CA-Unicenter tool. Bank may at its discretion require solution provider to integrate the Log Management And Event Correlation, DAM and VM tool with existing Adventnet/CA Unicenter and its components or any other ticket systems available in Bank including future versions at no extra cost to the Bank.

4.7.5 Comprehensive Log Management, Event Correlation, Database activity Monitoring and Vulnerability Management Solutions- Hardware & software integration

Successful bidder should integrate all the Hardware and software components supplied under this RFP.

4.7.6 Integration with all devices/applications/databases to be monitored

Successful bidder will be required to integrate all the devices supplied as part of this RFP as well as all the Bank's devices/applications/databases with the proposed solution.

4.7.7 Development of Connectors for customized applications/devices

While it is expected that connectors for all the standard applications and devices will be readily available in the collector and Log management devices, connector for mostly in- house/custom built applications will need to be developed. The team deployed for integration of Log Management And Event Correlation/DAM/VM tools will be expected to develop connector applications without any additional cost for the custom built applications specifically developed for Indian Bank.

4.7.8 Proof of concept for Proposed Solution as per RFP

Bank may at its discretion ask all the technically qualified bidders to carry out Proof of Concept(POC) of the proposed solution as mentioned in the tender to the Bank at Bank's premises and demonstrate the entire solution capability for the following Use cases.

- Use Cases for Internet Banking Transactions
- Use Cases for ATM Transactions
- Use Cases for RTGS / NEFT Transactions
- Use Cases for CBS System

- Use cases for Anti Money Laundering solution
- Any other use case as decided by the Bank

The POC should be completed within 5 business days (10 am to 6 pm) from the date of intimation

The bidder should bring all the relevant infrastructure for Proof of Concept.

Bank reserves the right to reject the solution, if not satisfied with the proof of concept testing and if the bidder's ability to work with the existing infrastructure is too limited or difficult to manage and is not in the interest of the Bank to consider the solution. All decisions taken by the Bank during evaluation is final.

4.7.9 Training for identified Bank's officials

Successful bidder must provide the detailed administrative training (5-7 officials), induction (15-20 officials) and refresher training (15-20 officials) for the entire solution as per the official OEM curriculum to the persons nominated by the Bank. The training should be arranged by the successful bidder at their own cost. The administrative training should be provided by OEM. All expenses related to training shall be borne by the successful bidder.

In addition to the above trainings, on site post implementation training should be provided to the identified Bank staff.

Successful bidder will also be expected to conduct onsite executive level sessions advising the features of solutions and monitoring of the events through the web based Dashboard.

The trainings should include the architecture, hardware, software, integration, customization, policy installation, trouble shooting, reporting and other aspects of the system. Vendor should ensure knowledge transfer and will involve the Bank officials during implementation of the solution as per scope of the project. Successful bidder shall provide comprehensive training manual, lecture notes, handouts and other training documentation during trainings. The persons in the above trainings may be different.

4.7.10 Workflow Automation

Selected vendor will define the work flow automation for the proposed solution so that applications are integrated and manual intervention is minimal.

4.7.11 Integration with the existing SOC Operations

Bank has a well-established captive SOC managed by a security service provider. SOC is also running an event correlation tool which correlates logs from Security devices alone and not from all the servers/applications/database logs.

Selected bidder will develop the work flow process for attending to the various functions of the Log Management and Event Correlation tool in consultation with the Bank and the SOC Service Provider including the work flow for attending to the incidents generated through the tools to be implemented. Bidder will also develop documents such as user manual, systems manual for smooth

functioning of tools delivered under this project.

Bidder will configure the Log Management And Event Correlation, DAM, VM tools and implement and integrate with existing Incident Management tools used in the Bank in consultation with the Bank and SOC Service Provider

Bank has the right to relocate any one or all the tools to different locations.

4.7.12 Deliverables

Successful bidder should supply and install all the hardware, software and peripheral components and supporting systems as per the bank's requirement under the scope of RFP
Successful bidder has to provide **an L2 Engineer** to maintain and manage the tools delivered under this project onsite between 9 am to 6 pm on all Bank's working days and within 3 hours between 6 pm to 9 am. L2 Engineer has to monitor the health of Hardware and software supplied by the bidder. Between 6 pm to 9 am, bidder can provide telephonic support to the Bank Officials and the existing Service Provider's SOC Team, if the problem can be resolved through telephonic support. If the problem has to be resolved through onsite support only, bidder has to provide onsite support within 3 hours from the time of call. Bank will decide about the type of support required, either onsite or offsite during the period between 6 pm and 9 am. The bidder will deliver the services and provide the reports to the Bank on periodic basis throughout the contract period for each of the services mentioned under project scope, in addition to providing other critical observations/methods/ improvements as deemed fit based on bidder's professional experience for each of the services mentioned above

Successful bidder should monitor and manage the tools delivered under this project as per the timings specified above. They should regularly fine tune the Log Management And Event Correlation, DAM and VM tools implementation to reduce false positives; Continuously assist in improving the SOC operations to maximize the usage of tools. It should manage archival of logs as per the archival and retention policy of the Bank. They should conduct vulnerability management scanning of integrated IPs using supplied VM Tool as per Bank's requirements and submit report to bank with remedies.

Successful bidder should provide role based access to dashboard. It should provide secure web based incident management and dashboard facility to enable Bank and SOC Service Provider to monitor the incidents status with drill down facility on various parameters.

Successful bidder should provide comprehensive training as defined above under point no: 4.7.9. Provide the complete set of Operation and System Manuals in -3- sets of hardcopies as well as in softcopies of all the systems/components provided as part of the implementation.

Successful bidder should define the process manual for all the tools provided.

Commercial tools should be provided for all the solutions and freeware tools should not be provided.

Successful bidder should provide **24X7X365** comprehensive maintenance support (all parts inclusive) at DC and DR to resolve any technical problem/issues.

The L2 onsite Engineer should be product certified for solution provided. The engineer should be responsible for managing the entire solution provided under the project on day to day basis and ensure uptime of entire solution. The Engineer should take periodic **Hot/Online Backup** without affecting any system as per bank's backup policy. During Disaster at DC or during DR Drill activity the engineer should be available at DR Site till normalcy is restored.

4.7.13 Backups

The Solution should have provision of taking HOT/ONLINE backup in Tape Library provided by the bidder without affecting any system performance with periodicity as per bank's backup/archiving policy.

4.7.14 Service Level Agreement

Solution Uptime (Hardware/Software/devices/components)

Note: If any penalties levied during the 1st year post Implementation and before AMC starts, the same may be adjusted with the pending payments, if any and subsequent AMC Payments. In case of penalties during any quarter of AMC period overshoots the quarterly AMC amount, the same will be adjusted with subsequent quarterly AMC payments.
.
Bank reserves the right to invoke performance guarantee in case of need, at Bank's discretion.

SL. No.	Service Area	Service Level	Penalty
1	Device(Hardware/Software) component Failure	Problem should be resolved within 3hours	Nil
		Problem resolved between 3 to 24 hours.	0.1% of Total Capital Cost or 3% equivalent of Quarterly AMC cost whichever is higher for each such failure during the quarter subject to maximum of 2 % of Total capital cost for the quarter.
		Problem resolved between 24 to 48 hours.	0.2% of Total Capital Cost or 6% equivalent of Quarterly AMC cost whichever is higher for each such failure during the quarter subject to maximum of 2% of Total capital cost for the quarter.
		Problem resolved	0.4% of Total Capital

		between 48 to 72 hours.	Cost or 12% equivalent of Quarterly AMC cost whichever is higher for each such failure during the quarter subject to maximum of 2% of Total capital cost for the quarter.
		Problem resolved between 3 days to 7 days.	0.8% of Total Capital Cost or 25% equivalent of Quarterly AMC cost whichever is higher for each such failure during the quarter subject to maximum of 2% of Total capital cost for the quarter.
2	Set of Devices (Hardware/Software) component failure in HA mode leading to the complete disruption of the objective performed by the said devices		0.2% of Total Capital Cost or 6% equivalent of Quarterly AMC cost whichever is higher for each such failure during the quarter subject to maximum of 2 % of Total capital cost for the quarter.
3	Solution Uptime	Uptime % calculated on monthly basis Expected Monthly uptime=no of days in month*24*60*60 seconds.	
		99.5% and above	Nil
		98%to 99.49%	0.5% of Total Capital Cost or 15% equivalent of Quarterly AMC cost whichever is higher for each such failure during the quarter.
		95%to 97.99%	1% of Total Capital Cost or 30% equivalent of Quarterly AMC cost whichever is higher for each such failure during the quarter.
4	Onsite L2 Engineer	Availability on all Bank's working Days	Rs 1000/- per Day on non availability.

4.7.15 Project Team Members

- The key persons identified by the successful bidder for implementation should necessarily possess the requisite qualification/experience along with product certification or implementation experience of the proposed solution. The information should be shared with bank before starting of implementation of solution.
- Should have in-depth knowledge of IT and Banking processes with a minimum of three years' work experience in Information Security.
- Should have knowledge of legal and Regulatory requirements towards analyzing and handling security incidents.
- Should be certified in usage of tools to be implemented by the respective **OEM/Vendor.**
- Should have experience in implementing such tools.

4.7.16 Substitution of Project Team Members

During the assignment, the substitution of key staff identified for the assignment will not be allowed by the Bank unless such substitution becomes unavoidable to overcome the undue delay or that such changes are critical to meet the obligation. In such circumstances, the selected Bidder, as the case may be, can do so only with the prior written concurrence of the Bank and by providing the replacement staff of the same level of qualifications and competence. If the Bank is not satisfied with the substitution, the Bank reserves the right to terminate the contract and recover whatever payments(including past payments and payment made in advance) made by the Bank to the selected Bidder during the course of the assignment pursuant to this RFP. However, the Bank reserves the unconditional right to insist to the selected Bidder to replace any team member with another with the qualifications and competence as required for this project by the Bank during the course of assignment pursuant to this RFP.

4.7.17 Provision of Realtime alerts

Entire Proposed solution should have realtime alert mechanism through dashboard/SMS/ticketing system for hardware/software failures, supplied by the bidder.

SECTION 5

QUALIFICATION CRITERIA FOR BIDDERS

5. QUALIFICATION CRITERIA FOR BIDDERS

SL. No	Qualification Criteria	Supporting Documents	Compliance Status (Complied/Not Complied)
1.	The bidder should be A registered corporate in India registered under the Companies Act, 1956 and should be registered under CST and/or have the sales tax registration in the State where the company has registered office. Or A company/statutory body owned by Central/State Government.	The bidder should submit copy of : (1) Valid sales tax/VAT registration certificate (2) Service Tax Registration Certificate (3) Certificate of incorporation The bidder should submit its profile in the format as given in Section 9.3	
2.	The bidder's minimum average yearly turn over through Indian operations during its last three financial years should be at least Rs.25 crores.	Copies of attested/ audited Balance Sheet and Financial Information under Bidders Profile-Section 9.3 without any changes.	
3.	The bidder should have earned net profit during its last three financial years.	Copies of attested/ audited Balance Sheet and Financial Information under Bidders Profile-Section 9.3 without any changes.	
4.	The bidder should have been in existence in India for minimum of five years as on 31.3.2012.	Copy of Certificate of Incorporation	
5.	The Bidder should have experience in designing, installing, configuring, customizing and operating an Security Operations Center (SOC) and deployment of the proposed Log Management And Event Correlation, Database Activity Monitoring & Vulnerability Management Solutions with at least 250 devices (or) 5000 Events per Second (EPS.) The bidder should provide at least two client references for Comprehensive Log Management and Event Correlation, out of which at least one	Details (Service details) along with the name of the Organization, Year and Cost of the project, Contact person, and Contact numbers. Copies of documents in support of these projects, the certificate of commissioning Log Management And Event Correlation & DAM solutions from the clients. The details of these projects including site	

SL. No	Qualification Criteria	Supporting Documents	Compliance Status (Complied/Not Complied)
	should be in India and one should be with any financial institution. One reference must be of deployment of proposed solution by bidder/OEM (**in case of OEM reference, the deployment should be taken care by OEM. An assurance letter from OEM for installation needs to be submitted to bank along with other document)**. The bidder can also quote its own managed SOC used for providing Managed Security Services to its clients. If the bidder is serving more than 1 client from its own SOC, it will be treated as 1 citation only. The Bidder/OEM must provide 2 references for successful installation of DAM and 2 references for successful installation of VM anywhere in India or outside India.	addresses, names and telephone numbers of persons to be contacted for reference purpose should be submitted as per the format given in Section 9.4,. Bank will hold the right to visit such projects and verify with the clients in this regard and the bidder must facilitate such visits / verifications within India.	
6.	Bidder must have service support at **Chennai and Hyderabad**.	List of Service Locations duly signed by the Authorized Signatory. (Copy of latest Telephone bill of the Service locations to be enclosed)	
7.	The bidder should be Original manufacturer of product or the premium partner of the equipment manufacturer / software provider. The bidder, on successful bid, must be in a position to provide support/maintenance/upgradation during the period of contract with the Bank. In case of authorized partner, a letter of authorization to this effect from Original Supplier must be furnished as per the format given in Section 9.2 without any changes.	Manufacturer's Authorization form as per format 9.2 without any changes.	
8.	The bidder shall submit a letter of undertaking that they are currently not in the blacklisted of the Central/any of the State Governments in India or any Financial Institution in India or any of the its clients it is currently serving.	Self Declaration	

SL. No	Qualification Criteria	Supporting Documents	Compliance Status (Complied/Not Complied)
9.	The Bidder must possess ISO 27001 certification.	Copy of the certification duly attested by the authorized signatory and the certification must be valid at the time of submission of bid.	
10.	The Bidder should have adequate skilled personnel holding proposed product training certification with knowledge and technical expertise in handling the proposed Log Management And Event Correlation, DAM and VM solutions. At least 2 personnel should be having adequate experience & expertise in the relevant field with CISA/CISM/CISSP/CCNP and Certifications in the proposed solution.	List of the personnel with copies of their relevant product training certification	
11	Proposed Product should be in the leaders' quadrant/category as per Gartner or Forrester report published within the last three years and should not be under visionaries or niche players' category currently. A copy of the press release to this effect to be provided.	Please provide copy of such reports	
12	The bidder should be empanelled with CERT-In for Information Security services.		
13	The entire solutions should have road map for 5 years and necessary documentary evidence for road map and the support from OEM must be provided		

The eligibility will be seen based on the above criteria and the bank has the right to reject responses not meeting the qualification criteria.

SECTION 6

INSTRUCTIONS TO BIDDERS

6. INSTRUCTIONS TO BIDDERS

The Bidder is expected to examine all instructions, forms, terms and specifications given in the Bidding Documents. Failure to furnish all information required by the Bidding Documents may result in the rejection of its bid and will be at the Bidder's own risk. Bank will not be responsible for the same. Bids submitted by bidders without DD for Rs.10,000/- will be liable for rejection.

6.1 Pre Bid Meeting

6.1.1 Pre-bid Meeting will be held on 12.09.2012 at 11.30 A.M. at the following address to clarify the queries raised by the bidders.

Indian Bank
Head Office
Technology Management Dept
66 Rajaji Salai
Chennai – 600 001

6.1.2 Prospective bidders are requested to attend the Pre-bid Meeting. Bidder's designated representatives (maximum two persons) may attend the pre-bid meeting. The bidders are requested to send all their queries **two days** before the date of pre-bid meeting. Clarifications will be given for queries received in writing. The replies to the clarifications will be ported on the Indian Bank's Website. No queries will be entertained after pre-bid meeting

6.1.3 Amendment of bidding documents

At any time prior to the deadline for submission of bids, the Bank, for any reason, whether at its own initiative or in response to a clarification requested by a prospective Bidder, may modify the Bidding Documents by amendment.

All prospective bidders, will be notified of the amendment and it will be binding on them.

Amendments if any, will be ported in our Bank's Website.

6.2 DOCUMENTS CONSTITUTING THE BID

6.2.1. The Bid prepared by the Bidder should comprise the following components :

6.2.2. ***TECHNICAL BID*** – ***Part I*** - Sealed cover with superscriptions as " **Technical Bid**– "**Implementation of a Comprehensive Log Management, Event Correlation, Database Activity Monitoring & Vulnerability Management Solutions**" . .

6.2.3. ***COMMERCIAL BID – Part II –***Through Online Reverse Auction(Commercial details as per Annexure 9.8 should be submitted after completion of online reverse auction).

The envelope containing the Part-I *should* be placed in another envelope along with the DD for Rs 10,000- towards the Cost of the Bid Document and Bank Guarantee being the Bid Security for Rs. 10,00,000/ with the superscription :

"BID FOR Implementation of a Comprehensive Log Management, Event Correlation, Database Activity Monitoring & Vulnerability Management Solutions"– NOT TO BE OPENED BEFORE 27.09.2012 - 16.00 Hrs"

6.2.4. In addition to the Hard copy of the documents, a soft copy of the technical bid is also to be submitted. In case of any inconsistency between the soft and hard copies, the details in the hard copy only will prevail.

Any bid document not conforming to any one of the above terms will be liable for rejection.

6.3. TECHNICAL BID

i) Validity period of the bid – 180 days from the last date for submission of the bid.

ii) The bidders are expected to examine all terms and instructions included in the Documents. Failure to provide all requested information will be at bidders own risk and may result in the rejection of the proposal.

iii) BID FORM, PRICE SCHEDULES AND OTHER FORMATS are given in Section 9 .

iv) The bidder should submit all the specifications with their compliance level as applicable and remarks along with relevant documents wherever applicable and other requirements given in the Bid Document and Scope of Work.

v) The bidder should quote only one solution in the Bid and shall not quote for more than one solution in the same bid. Doing so may lead to disqualification of bid.

vi) The bidder should provide complete solution document. This document must include following details:

a). Architecture of the solution: This must contain details of implementation methodology of the project viz., Deployment of all the solutions with proposed time frame for the project.
b). Product details
c). Documentation of the products (software/hardware) to be deployed in the Solution along with Data Sheets, Details of Part Number and Fact Files pertaining to the appliances being quoted.
d). Details of OEM, a copy of authorization/undertaking letter from them for support and maintenance.
e). Any other details bidder wishes to provide.

In absence of any of above documents, the bid will be liable for rejection. The technical proposal must not include any details of commercial bid. Any bid consisting of Commercial information either in hard copy or soft copy will be liable for rejection.

6.4. COMMERCIAL BID AND GENERAL EVALUATION

The price should be quoted in the format attached to this bid after completion of online reverse auction for commercials (Format under section-9.8)

i) The commercial bid should list all the costs associated with the Assignment.
ii) The price should be firm, inclusive of all taxes, charges and duties payable etc. but exclusive of Octroi and Entry Tax.
iii) TDS as per rules, if applicable, will be deducted from the amount quoted.
iv) The Bank (Purchaser) will examine the quote to determine whether they are complete, whether the documents have been properly signed and whether the quote is generally in order.
v) The Bank (Purchaser) may waive any minor informality, non-conformity, or irregularity in a quote which does not constitute a material deviation.
vi) Prior to the detailed evaluation, the Bank (Purchaser) will determine the substantial responsiveness of quote documents. For the purposes of these Clauses, a substantially responsive quote is one which conforms to all the terms and conditions of the quote Documents without material deviations.
vii) Bank reserves the right to negotiate the price with the Lowest Quoted (L1) Bidder under exceptional circumstances before awarding the contract.
viii) The L1 bidder should submit a self declaration letter stating that they have not been blacklisted during the tender process before issue of Purchase order by the Bank. In case of blacklisting, the Purchase order may not be awarded.
ix) Bank will go for the reverse auction for commercial bid. Terms and conditions of the reverse auction will be communicated to the technically qualified Bidders prior to the commencement of the reverse auction exercise.

6.5. AWARD OF CONTRACT

6.5.1. Within 15 days from the date of receipt of award notification, the bidder should sign the contract as per the format furnished herewith (Section 9.6 ,).

6.6. BID SECURITY (EARNEST MONEY DEPOSIT)

6.6.1. The Bidder should furnish, as part of its bid, a bid security in the form of a bank guarantee issued by a scheduled commercial bank located in India, in the form provided in the Bidding Documents (Section 9.5) for a sum of Rs.10,00,000/- and valid for sixty (60) days beyond the validity of the bid. (i.e. Bid validity 180 days + 60 days = 240 days from the last date of the bid submission)

6.6.2. Unsuccessful Bidders' bid security will be discharged or returned within 30 days after the expiry of validity of the bid. The successful Bidder's bid security will be discharged upon the Bidder signing the Contract and furnishing the performance security.

6.6.3. The bid security may be forfeited if :

A Bidder withdraws its bid during the period of bid validity specified by the Bidder on the Bid Form or in the case of a successful Bidder, if the Bidder fails to sign the contract within the specified time of 15 days, or to furnish performance security.

6.7. PERIOD OF VALIDITY OF BIDS

Bids should remain valid for the period of 180 days after the last date for submission of bid prescribed by the Bank. A bid valid for a shorter period shall be rejected by the Bank as non-responsive.

6.8. FORMAT AND SIGNING OF BID

- All pages of the bid, except for unamended printed literature, shall be initialled by the person or persons signing the bid.

- Any interlineation, erasure or overwriting shall be valid only if they are initialled by the person or persons signing the Bid.

6.9. SEALING AND MARKING OF BIDS

The Bidder shall keep the DD for Rs 10,000/- favoring Indian Bank being the Cost of Bid document and Bid security, in the form of Bank Guarantee for Rs. 10,00,000/-, along with the Technical bid. Commercial Bid will be done through reverse auction.

The envelope containing the Part-I should be placed in an envelope with the superscription ""Implementation of a Comprehensive Log Management, Event Correlation, Database Activity Monitoring & Vulnerability Management Solutions" – NOT TO BE OPENED BEFORE 27.09.2012 - 16.00 hours"

The sealed outer envelope along with the cost of the bid document and Bid Security shall be addressed to the Bank at the address given below:

Assistant General Manager
Indian Bank, Corporate Office,
Expenditure Department
254-260, Avvai Shanmugham Salai,
Royapettah, Chennai 600 014, India

6.10. LAST DATE FOR SUBMISSION OF BIDS

Last Date for bid submission is: 1600 Hours on 27.09.2012

- In the event of the specified date for the submission of bids being declared a holiday for the Bank, the bids will be received up to the appointed time on the next working day.

- The Bank may, at its discretion, extend this deadline for the submission of bids by amending the Bid Documents, in which case all rights and obligations of the Bank and Bidders previously subject to the deadline will thereafter be subject to the deadline as extended.

- Any bid received by the Bank after the deadline for submission of bids prescribed by the Bank will be rejected and returned unopened to the Bidder.

6.11. OPENING OF TECHNICAL BIDS BY BANK

- The Bank will open the Part I of the bid (Technical bid) in the presence of officers authorised for the purpose, and bidders' representatives at 16.30 hours on 27.09.2012. No bid shall be rejected at bid opening, except for late bids, which shall be returned unopened to the Bidder.

- The Bank will inform the agency and reverse auction details to bidders who are found eligible on evaluation of Technical Bid.

- Bank will go for the reverse auction for commercial bid. Terms and conditions of the reverse auction will be communicated to the eligible Bidders prior to the commencement of the reverse auction exercise.

6.12. CLARIFICATION OF BIDS

During evaluation of the bids, the Bank may, at its discretion, seek clarification from the Bidder with regard to the bid. The request for clarification and the response shall be in writing.

6.13. EVALUATION METHODOLOGY

1. The Bank will examine the bids to determine whether they are complete, whether required sureties have been furnished, whether the documents have been properly signed, and whether the bids are generally in order.

2. The Bank at its discretion may modify any minor criteria in the bid, which does not affect the relative ranking of any Bidder.

3. Prior to the detailed evaluation, the Bank will determine the substantial responsiveness of each bid to the bidding documents. For purposes of these Clauses, a substantially responsive bid is one which conforms to the terms and conditions of the qualification criteria and the Bidding Documents without material deviations.

4. If a bid is not substantially responsive, it will not be considered by the Bank and may not subsequently be made responsive by the Bidder by correction of the non-conformity.The bid / in such case.

5. The Bank will evaluate and compare the bids, which have been determined to be technically responsive and acceptable.

6. Bids will be short-listed based on the qualification criteria, all the criteria specified in the technical bid. First, Technical bid documents will be evaluated for fulfillment of eligibility criteria. Technical bids of only those Bidders who fulfill the eligibility fully as per Qualification Criteria will be taken up for further evaluation/selection process rejecting the bids which are not qualifying.

7. The Bank expects all the requirements and specifications given in Section 8 to be complied. Non-compliance in any one of them will lead to disqualification. Maximum of 2 features under each Major head can be permissible for customization.The customisation must be inclusion of the functionality as a

software/hardware attachment without changing the main characteristics of the product and must be completed within the period of implementation of solution. Any features which are not readily available as well as non customizable will be liable for rejection.

8. The evaluation of technical proposals, among other things, will be based on the following:

   - Prior experience of the Bidder in undertaking projects of similar nature.
   - Professional qualifications and experience of the key Staff proposed/ identified for this assignment.
   - Methodology/Approach proposed for accomplishing the proposed project, Proof of Concept testing/ Activities / tasks, project planning, resource planning, effort estimate etc.

   Various stages of technical evaluation are given below:

   1. Eligibility evaluation as per the criteria prescribed in Section 5- Qualification Criteria.
   2. Evaluation of technical proposals of Bidders qualified in eligibility evaluation, based on response and presentation by the bidder.
   3. Bank may at its discretion ask the bidders to demonstrate POC for the proposed solution as per section 4.7.8.

   Presentation-cum-Interview

   The Bidders who are qualified in eligibility evaluation, have to give presentation/interactions before panel of representatives of the Bank on the methodology/ approach, time frame for various activities, strengths of the Bidders in carrying out the tasks as per the RFP. The technical competence and capability of the Bidder should be clearly reflected in the presentation. If any short listed Bidder fails to make such presentation, he will be eliminated from the evaluation process. Bank may at its discretion seek from the Bidder to conduct proof of concept testing of the solution being provided to the Bank.

9. Bank will go for the reverse auction to decide the L1 bidder.

10. The comparison shall be between the prices quoted(Capital Cost –Inclusive of all taxes and duties and exclusive of Octroi and Entry Tax, AMC Cost- inclusive of all taxes but exclusive of service taxes) for the entire project requirement for 5 Years as per RFP and the bidder who has quoted the lowest during the reverse auction will be awarded the contract.

11. Any effort by the bidder to influence the purchaser in the process of evaluation of bids and in decisions concerning award of the contract will result in the rejection of their bid.

12. Any bid which does not qualify in any of the points mentioned in the qualification criteria or any of the criteria mentioned in the Technical Bid will be technically rejected and all those who qualify on all the criteria will be considered for further evaluation.

6.14. BANK'S RIGHT TO ACCEPT ANY BID AND TO REJECT ANY OR ALL BIDS

The Bank reserves the right to accept or reject any bid, and to annul the bidding process and reject all bids at any time prior to award of contract, without assigning any reason therefor and without thereby incurring any liability to the affected Bidder or Bidders.

6.15. SIGNING OF CONTRACT

- At the same time as the Bank notifies the successful Bidder that its bid has been accepted, the Bank will send the Bidder the Contract Form provided in the Bidding Documents, incorporating all agreements between the parties. A separate Non disclosure Agreement will also be entered into between the Bank and the Bidder along with the signing of contract.
- Within 15 (fifteen) days of receipt of the Contract Form, the successful Bidder shall sign and date the Contract and return it to the Bank.

6.16. PERFORMANCE SECURITY

- Within 10 (ten) days of the signing of contract, the successful Bidder shall furnish the performance security equivalent to 10% of the total contract amount valid for a period of **66 months** in the form of a Bank Guarantee in accordance with the Conditions of Contract, in the Performance Security Form provided in the Bidding Documents.

- Failure of the successful Bidder to comply with the requirement of signing of contract and performance Security shall constitute sufficient grounds for annulment of the award and forfeiture of the bid security.

6.17. NEGOTIATION

- Bank reserves the right to negotiate with lowest bidder for further reduction in price under exceptional circumstances.

SECTION 7

CONDITIONS OF CONTRACT

7. CONDITIONS OF CONTRACT

7.1. DEFINITIONS

In this contract, the following terms shall be interpreted as indicated:

a. "**Applicable Law**" means the laws and any other instruments having the force of law in India.

"**Bank**" means INDIAN BANK.

"Contract" means the agreement entered into between the Bank and the successful bidder, as recorded in the Contract Form signed by the parties, including all the attachments and appendices thereto and all documents incorporated by reference therein;

"**Contract Price**" means the price payable to the successful bidder under the Contract for the full and proper performance of its contractual obligations;

"**Goods**" means all of the deliverables or other materials which the bidder should deliver as per this contract;

"**Party**" means the Bank or the bidder, as the case may be and Parties means both of them.

"**Personnel**" means persons who are the employees of the successful bidder and assigned to the performance of the Services or any part thereof.

"**Project Site"**, where applicable, means the places that were mentioned in the Scope of Work.

"**Services**" means those services ancillary to the deliverables of the bidder covered under the Contract.

"**Purchaser**" means Indian Bank.

7.2. LAW GOVERNING THE CONTRACT

This Contract, its meaning and interpretation, and the relation between the Parties shall be governed by the Applicable Law.

The Contract shall be interpreted in accordance with the laws of India and any other guidelines having the force of law in India.

7.3. LANGUAGE

The contract to be executed in English which shall be the binding and controlling language for all matters relating to the meaning or interpretation of the contract.

7.4. ADDRESS FOR COMMUNICATION

The address of the Bank is:

Assistant General Manager (TMD/ISSC)
INDIAN BANK,
Technology Management Department
66, Rajaji Salai
Chennai 600 001

7.5. STANDARDS

The products and systems supplied under this Contract shall conform to the standards mentioned in the Technical Specifications

7.6. CONTRACT AMENDMENT

No variation in or modification of the terms of the Contract shall be made except by written amendment to the Contract signed by the parties.

7.7. SETTLEMENT OF DISPUTES

7.7.1. If any dispute or difference of any kind whatsoever shall arise between the bank and the Successful bidder in connection with or arising out of the contract, the parties shall make every effort to resolve amicably such disputes or difference by mutual consultation.

7.7.2. If after 30 days the parties have failed to resolve their disputes or difference by such mutual consultation, then either the bank or the Successful bidder may give notice to the other party of its intention to commence arbitration, as hereinafter provided, as to the matter in dispute, and no arbitration in respect of this matter may be commenced unless such notice is given.

7.7.3. Any dispute or difference in respect of which a notice of intention to commence arbitration has been given in accordance with this clause shall be finally settled by arbitration. Arbitration may be commenced prior to or after delivery of the goods under the contract.

Arbitration proceedings shall be conducted in accordance with the following rules of Procedure.

The dispute resolution mechanism to be applied shall be as follows:

(a) In case of dispute or difference arising between the Bank and the Successful bidder relating to any matter arising out of or connected with this agreement, such dispute or difference shall be settled in accordance with the Arbitration and Conciliation Act, 1996. The arbitral tribunal shall consist of 3 arbitrators one each to be appointed by the Bank and the Successful bidder; the third Arbitrator shall be chosen by the two Arbitrators so appointed by the Parties and shall act as Presiding Arbitrator. In case of failure of the two arbitrators appointed by the parties to reach upon a consensus within a period of 30 days from the appointment of the Arbitrator appointed subsequently, the Presiding Arbitrator shall be appointed by the Indian Banks' Association, India which appointment shall be final and binding on the parties.

(b) If one of the parties fails to appoint its arbitrator within 30 days after receipt of the notice of the appointment of its Arbitrator by the other party, then the Indian Banks' Association shall appoint the Arbitrator. A certified copy of the order of the Indian Banks' Association making such an appointment shall be furnished to each of the parties.

(c) Arbitration proceedings shall be held at Chennai, India, and the language of the arbitration proceedings and that of all documents and communications between the parties shall be English.

(d) The decision of the majority of arbitrators shall be final and binding upon both parties. The cost and expenses of Arbitration proceedings will be paid

as determined by the Arbitral Tribunal. However, the expenses incurred by each party in connection with the preparation, presentation etc. of its proceedings as also the fees and expenses paid to the arbitrator appointed by such party or on its behalf shall be borne by each party itself.

7.7.4. Notwithstanding any reference to arbitration herein,

a) the parties shall continue to perform their respective obligation under the contract unless they otherwise agree; and
b) the bank shall pay the Successful bidder any monies due to him as per the Contract Terms.

7.8. NOTICES

Any notice, request or consent made pursuant to this contract shall be in writing and shall be deemed to have been made when delivered in person to an authorized representative of the party to whom the communication is addressed, or when sent by registered mail, courier or facsimile to such party at the address specified above. A notice shall be effective when delivered or on the notice's effective date.

7.9. IMPLEMENTATION SERVICES

The Supplier shall provide all Services specified hereunder and in the Technical and functional specifications in accordance with the highest standards of professional competence and integrity. If the purchaser finds that any of the staff of the supplier assigned to work at the purchaser site is not responsive then the supplier will be notified, the supplier should resolve the issue to the satisfaction of the purchaser.

7.10. USE OF CONTRACT DOCUMENTS AND INFORMATION

7.10.1. The Successful bidder shall not, without the Bank's prior written consent, disclose the Contract, or any provision thereof, or any specification, plan, drawing, pattern, sample or information furnished by or on behalf of the Bank in connection therewith, to any person other than a person employed by the Successful bidder in the performance of the Contract. Disclosure to any such employed person shall be made in confidence and shall extend only as far as may be necessary for purposes of such performance.

7.10.2. The Successful bidder shall not, without the Bank's prior written consent, make use of any document or information pertaining to this contract except for purposes of performing the Contract.

7.11. INDEMNIFICATION

7.11.1. The Supplier shall, at their own expense, defend and indemnify the Purchaser against all third-party claims of infringement of Intellectual Property Rights, including patent, trademark, copyright, trade secret or industrial design rights arising from use of the Products or any part thereof in the Purchaser's country.

7.11.2. The Supplier shall expeditiously extinguish any such claims and shall have full rights to defend itself therefrom. If the Purchaser is required to pay compensation to a third party resulting from such infringement, the Supplier shall be fully responsible therefor, including all expenses and court and legal fees.

7.11.3. As a condition precedent to the foregoing, the Purchaser will give notice to the Supplier of any such proceedings or claim without delay, shall provide reasonable assistance to the Supplier in disposing of the claim.

7.11.4. The Supplier shall have sole control on the conduct of such proceedings or claim and any negotiations for the settlement of any such proceedings or claim and the Purchaser shall provide the Supplier with the assistance, information, and authority reasonably necessary to perform the above and the Purchaser shall at no time admit to any liability for or express any intent to settle the claim.

7.12. SOFTWARE LICENSE AGREEMENTS

7.12.1. All the intellectual property rights and ownership of all tools, processes, software, utilities, and methodology including any Supplier proprietary products or components thereof used in the provision of Services and/or development of Products and all new ideas, inventions, innovations, or developments conceived, developed or made by Supplier or its consultants/employees thereto while providing the Services hereunder shall remain the sole and absolute property of Supplier, with full ownership rights therein ('Supplier Property'). Supplier shall grant in favor of Purchaser a non-exclusive, non-transferable, royalty-free, user license valid within the territory of India to use the Supplier Property to the extent they form part of the Products and will be required for the proper functioning of the Products.

7.12.2. Purchaser acknowledges that Supplier provides consulting, implementation, maintenance and development services to its other clients/purchasers and agrees that nothing in this Agreement shall be deemed or construed to prevent Supplier from conducting such business. Specifically Purchaser agrees that notwithstanding anything contrary herein Supplier shall have the right to (a) develop, use and distribute works that perform functions the same as or similar to the Products ; and (b) provide services same or similar to the Services either for itself or for its other clients and it will not infringe the proprietary rights of Purchaser in the Products subject to Supplier maintaining confidentiality of Purchaser proprietary and confidential information.

7.13. PERFORMANCE SECURITY

7.13.1. Within 10 (ten) days of signing of contract, the Successful bidder shall furnish to the Bank the performance security equivalent to 10% of the total contract amount valid for a period of **66 months** in the form of a Bank Guarantee in the format enclosed (Section 9.7) from the date of acceptance of Purchase Order.

7.13.2. The proceeds of the performance security shall be payable to the Bank as compensation for any loss resulting from the Successful bidder's failure to complete its obligations under the Contract.

7.13.3. The performance security will be discharged by the Bank and returned to the Successful bidder not later than thirty (30) days following the date of completion of the Successful bidder's performance obligations under the Contract, including any obligations under warranty.

7.14. PAYMENT TERMS

The Bidder's request(s) for payment shall be made to the Bank in writing, accompanied by an invoice describing, as appropriate, the Goods delivered and services performed and by documents submitted, and upon fulfilment of other obligations stipulated in the Contract.

Bank will release the payment within 30 days of receipt of the undisputed invoice, after deduction of any charges such as penalties etc., No advance payments will be made. Further, it may be noted that the mentioned criteria is only for the purpose of effecting agreed price payment. The selected Bidder shall cover the entire scope including deliverables mentioned in Section II.

The following documents are to be submitted for claiming payment:

i) Supplier's original invoice showing order number, goods description, quantity, unit price and total amount.
ii) Delivery Note/Challan showing the full details of the consignment acknowledged by Bank officials.
iii) A copy of insurance certificate in respect of hardware.
iv) Manufacturer's/Supplier's warranty certificate
v) Inspection certificate issued by the nominated inspection agency, if any.

Payment shall be made directly into the successful bidder's bank account. The successful bidder has to share its bank account details for payment.

The payment terms are as below: For phases, please refer to para 7.30-Time frame for completion of the project

Note : The successful bidder must submit BILL OF MATERIALS along with costs for each line items within a day from date of declaration of L1 bidder.

S.NO.	Description	Payment Terms (Please refer Section7.30 for Various Phases)
1	Centralized Logger and Event Correlation Solution components	50% against delivery, installation. 20% after completion of Phase I and basic User acceptance test. 20% after completion of Phase II 10% after end of warranty period.
2	DAM Solution	50% against delivery, installation. 20% after completion of Phase I and basic User acceptance test. 20% after completion of Phase II. 10% after end of warranty period.
3	VM Solution	50% against delivery, installation. 40% against successful integration and User acceptance test. 10% after end of warranty period.

4	Storage, Tape Library,	50% against delivery. 40% against successful installation 10% after end of warranty period.
5	Standard Perforated Racks, Accessories and others etc.	80% on delivery and 20% on installation.
6	AMC	Quarterly basis after expiry of the quarter(in arrears). AMC will start after warranty.

Invoices must be raised separately as per above mentioned line items. All payments will be made on successful completion of the job to the satisfaction of the Bank and achievement of the objective as defined in the scope of work after deducting any penalty which may be chargeable irrespective of the invoice being paid.

7.15. PRICES

Prices payable to the Supplier as stated in the Contract shall be firm and not subject to adjustment during performance of the Contract.

7.16. OBLIGATIONS OF THE SUPPLIER

7.16.1. The Supplier will abide by the job safety, insurance, customs and immigration measures prevalent and laws in force in the Purchaser's country, and will indemnify the Purchaser from all demands or responsibilities arising from accidents or loss of life or property, the cause of which is the Supplier's negligence. The Supplier will pay all indemnities arising from such incidents and will not hold the Purchaser responsible or obligated.

7.16.2. The Supplier is responsible for, and obligated to conduct all contracted activities with due care and diligence, in accordance with the Contract, and using state-of-the-art methods and economic principles, and exercising all reasonable means to achieve the performance specified in the Contract.

7.16.3. Confidentiality - The successful bidder either during the term or after the expiration of this contract shall not disclose any proprietary or confidential information relating to the project, the services, this contract, or the client's business or operations without the prior written consent of the client. A separate non-disclosure agreement shall be executed by the supplier (L1 bidder), the format for which is provided under 9.11.

The supplier has to agree for

- RBI or persons authorized by it to access the records and to cause inspection.

- o Maintaining Confidentiality of customer information even after the completion of contract.

- o Obtention of prior approval of the bank for use of subcontractors for outsourced activity etc.

7.16.4. Reporting obligations - The bidder shall submit to the client the reports and other accounts specified in deliverables within the time limit set forth.

7.17. DELIVERY AND DOCUMENTS

7.17.1. Delivery and Installation of the Appliances (hardware/ software systems) shall be made by the Supplier in accordance with the requirements in the RFP.

7.17.2. The Supplier should produce 2 Copies of Supplier's Invoice showing contract number, products description, quantity, unit price and total amount to the purchaser (Delivery Challan and getting it acknowledged by Bank officials to be mentioned)

7.17.3. The purchaser will do a verification/audit of the deliverables mentioned in the RFP to ascertain that the deliverables conform to the specifications and requirements of the purchaser.

7.17.4. DOCUMENTS PREPARED BY THE BIDDERS FOR THIS PURPOSE TO BE THE PROPERTY OF THE BANK

All plans, drawings, specifications, designs, reports and documents submitted by the bidder shall become and remain the property of the Bank and the bidder shall, upon termination or expiration of this contract, deliver all such documents to the Bank together with a detailed inventory thereof. The bidder may retain a copy of such documents. The bidder shall not use these documents for purposes unrelated to this contract without the prior written approval of the client.

7.18. DELAYS IN THE SUPPLIER'S PERFORMANCE

7.18.1. Delivery and installation of the Systems and performance of Services shall be made by the Supplier in accordance with the time schedule mutually agreed by the parties and set out in the Contract.

7.18.2. If at any time during performance of the Contract, the Supplier or its subcontractor(s) should encounter conditions impeding timely delivery of the Systems and/or performance of Services, the Supplier shall promptly notify the Purchaser in writing of the fact of the delay, its likely duration and its cause(s). After receipt of the Supplier's notice, the Purchaser shall evaluate the situation and may at its discretion extend the Supplier's time for performance in which case the extension shall be ratified by the parties by amendment of the Contract.

7.18.3. A delay by the Supplier in the performance of its delivery obligations due to reasons solely and directly attributable to the Supplier alone and that was in no way contributed to by any act or omission of the Purchaser or any event of force majeure shall render the Supplier liable to the imposition of liquidated damages, unless an extension of time is agreed upon without the application of liquidated damages.

7.19. LIQUIDATED DAMAGES

7.19.1. If the Successful bidder fails to perform the Services within the period(s) specified in the Service Level Agreement **(SLA),** the Bank shall, without prejudice to its other remedies under the Contract, deduct penalty from the Contract Price, as liquidated damages, for every such default in service. (SLA will be provided along with the Purchase order)

7.19.2. If the Successful bidder fails to deliver any or all of the Goods or to perform the Services within the period(s) specified in the Contract, the Purchaser shall, without prejudice to its other remedies under the Contract, deduct from the Contract Price, as liquidated damages, a sum equivalent to 0.5% of the Invoice price of the Goods or unperformed Services for each week or part thereof of delay until actual delivery or performance, upto a maximum deduction of 10%. Once the maximum is reached, the Purchaser may consider termination of the contract. The date of delivery of last item to a location will be taken as the date of delivery for entire set of system to that location, for the purpose of calculation of Liquidated Damages.

7.19.3. At that point the contract price will stand reduced to the actual amount payable by the Bank. Proportionately the amount payable to the Successful bidder will also stand reduced. All the deliverables given to the Bank at that instant will continue to be the property of the bank and the bank may use the same for any purpose which it may deem fit.

7.20. TERMINATION FOR DEFAULT

7.20.1. The Bank, without prejudice to any other remedy for breach of contract, by written notice of default sent to the Successful bidder, may terminate this Contract in whole or in part :

a. if the Successful bidder fails to deliver any or all of the deliverables within the period(s) specified in the Contract, or within any extension thereof granted by the Bank; or
b. if the Successful bidder fails to perform any other obligation(s) under the Contract.
c. If the Successful bidder, in the judgement of the Bank has engaged in corrupt or fraudulent practices in competing for or in executing the Contract.
d. When the value of the liquidated damages exceed 10% of the contract amount as in clause 7.19

'For the purpose of this clause:

"corrupt practice" means the offering, giving, receiving or soliciting of any thing of value to influence the action of a public official in the procurement process or in contract execution; and

"**fraudulent practice**" means a misrepresentation of facts in order to influence a procurement process or the execution of a contract to the detriment of the Bank, and includes collusive practice among Bidders (prior to or after bid submission) designed to establish bid prices at artificial non-competitive levels and to deprive the Bank of the benefits of free and open competition.

7.20.2. In the event the Bank terminates the Contract in whole or in part, the Bank may procure, upon such terms and in such manner as it deems appropriate, Goods or Services similar to those undelivered, and the

Successful bidder shall be liable to the Bank for any excess costs for such similar Goods or Services. However, the Successful bidder shall continue performance of the Contract to the extent not terminated.

7.21. TERMINATION FOR INSOLVENCY

If the supplier becomes bankrupt or insolvent, has a receiving order issued against it, compounds with its creditors, or, if the supplier is a corporation, a resolution is passed or order is made for its winding up (other than a voluntary liquidation for the purposes of amalgamation or reconstruction), a receiver is appointed over any part of its undertaking or assets, or if the supplier takes or suffers any other analogous action in consequence of debt; then the Purchaser may at any time terminate the contract by giving written notice to the Supplier. If the contract is terminated by the Purchaser in terms of this Clause, termination will be without compensation to the Supplier, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to the Purchaser. In case the termination occurs before implementation in all the locations in terms of this clause, the puchaser is entitled to make his claim to the extent of the amount already paid by the purchaser to the supplier.

7.22. TERMINATION FOR CONVENIENCE

The Bank, by written notice sent to the Successful bidder, may terminate the Contract, in whole or in part, at any time for its convenience. The notice of termination shall specify that termination is for the Bank's convenience, the extent to which performance of the Successful bidder under the Contract is terminated, and the date upon which such termination becomes effective.

7.23. FORCE MAJEURE

7.23.1. The Successful bidder shall not be liable for forfeiture of its performance security, liquidated damages, or termination for default, if and to the extent that, its delay in performance or other failure to perform its obligations under the Contract is the result of an event of Force Majeure.

7.23.2. For purposes of this clause, "Force Majeure" means an event beyond the control of the Successful bidder and not involving the Successful bidder's fault or negligence and not foreseeable. Such events may include, but are not restricted to, acts of the Bank in its sovereign capacity, wars or revolutions, fires, floods, epidemics, quarantine restrictions, and freight embargoes.

7.23.3. If a Force Majeure situation arises, the Successful bidder shall promptly notify the Bank in writing of such condition and the cause thereof. Unless otherwise directed by the Bank in writing, the Successful bidder shall continue to perform its obligations under the Contract as far as is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.

7.24. WARRANTY

7.24.1. The supplier undertakes that

a) warranty shall remain valid for 12 months after the Appliances have been installed at the final destination indicated in the Contract, or for 18 months after the date of receipt of shipment at the destination, if the installation is delayed due to Bank, whichever period concludes earlier. This should be incorporated in the Invoice.

b) the deliverables supplied is complete in all respects as per the specifications responded in the bid.

c) the deliverables are verified for its correctness and in case of any error(s) the same will be rectified immediately or replaced.

d) they accept responsibility for the successful integration and interoperability of all proposed products/deliverables as required by the Bidding Documents.

e) all the deliverables offered, whether belonging to the bidder or any third party operate effectively and the Bidder is willing to accept responsibility for its successful operation.

7.24.2. The Supplier warrants, for the duration of the Warranty Period commencing from the date of implementation at all sites, that all the deliverables supplied under this Contract shall have no critical defect arising from design or from any act or omission of the supplier.

7.24.3. The Purchaser shall promptly notify the Supplier in writing of any claims arising under this warranty. Upon receipt of such notice, the Supplier shall, within the warranty period and with all reasonable speed rectify the mistake without costs to the Purchaser.

7.24.4. If the Supplier, having been notified, fails to remedy the defect(s) falling within the warranty obligations, the Purchaser may proceed to take such reasonable remedial action as may be necessary, at the Supplier's risk and expense and without prejudice to any other rights which the Purchaser may have against the Supplier under the Contract.

7.24.5. The Supplier warrants that there is no intention of discontinuing development / upgradation of the Products to be supplied under the Contract without written notification to the Purchaser. However, the products supplied will be continued to be supported as per the terms of contract.

7.24.6. Without limitation, the Supplier warrants that it shall secure all necessary written agreements, consents and transfers of rights from its employees and other persons or entities whose services are used in relation to the deliverables, including, a written agreement with employees that all deliverables created under the Contract fall within the scope of their employment duties,

7.24.7. During the Warranty Period, the Supplier will provide and arrange for installation at no additional cost to the Purchaser all Product and documentation updates and new software version releases, if any, within mutually agreed time of their availability .

7.24.8. Subject to the provisions of Indemnity clause 7.12., the Supplier hereby represents and warrants that the deliverables as delivered does not and will

not infringe any Intellectual Property Rights held by any third party and that it has all necessary rights, or at its sole expense shall have secured in writing all transfers of rights and other consents necessary to make the assignments, licenses and other transfers of Intellectual Property Rights and the warranties set forth in the Contract, and for the Purchaser exclusively to own or exercise all Intellectual Property Rights as provided in the Contract. Without limitation, the Supplier shall secure all necessary written agreements, consents and transfers of rights from its employees and other persons or entities whose services are used.

7.24.9. Without prejudice to the warranties given for individual Products or Services, the Supplier hereby warrants to the Purchaser that, subject to the provisions of clause 7.27.1:

a) The Systems represent a complete, integrated solution to the Purchaser's requirements as set forth in the Technical/Functional Specifications and will provide the functionality and performance set forth therein. The Supplier shall accept responsibility for the successful interoperation and integration in accordance with the requirements of the Technical / Functional Specifications, of all Products provided under the Contract; The supplier is responsible for ensuring that the operations of the deliverables conform to the requirements and the specifications.

b) The Systems' specifications, capabilities and performance characteristics are as stated in the Supplier's Bid and Product documentation.

c) The Supplier will offer all possible assistance to the Purchaser to seek warranty services or remedial action from subcontracted third party producers or licensors of Products included in the Systems. The Supplier will make all reasonable and necessary efforts to correct defects in the Systems that constitute significant deviations from the Technical Specifications and/or Supplier performance claims.

7.25. ANNUAL MAINTENANCE CONTRACT(AMC) / ANNUAL RECURRING LICENSE (ARL)

All the software patches, hardware and software components has to be replaced or upgraded at no extra cost to the Bank. AMC/ARL shall include consultancy, manpower and updation/upgrade of all past released/future versions of the software and migration from old to new version without any extra cost to the Bank. Any failure in any part of the systems supplied has to be replaced or upgraded at no extra cost while maintaining the service levels (SLA).

7.26. INFORMATION SYSTEM SERVICE AND SUPPORT

The Supplier is obliged to provide for maintenance and support services on 24X7 basis, as per the terms of this contract.

7.27. CHANGE ORDERS

7.27.1. The Purchaser may at any time, by a written order given to the Supplier make changes within the general scope of the Contract in any one or more of the following:

a) drawings, designs, or specifications, for Systems or for Services that are to be integrated, developed or customized specifically for the Purchaser;

b) place of delivery

c) the schedule for Installation or Acceptance

d) the Services to be provided by the Supplier; and / or

e) the substitution of new Products and Services from the Supplier. When such substitution is requested by the Purchaser, the Supplier shall notify the Purchaser in writing within 30 days of its decision to accept or reject the proposed Change Order.

7.27.2. If any such change causes an increase or decrease in the cost of, or the time required for, the Supplier's performance of any provisions under the Contract, an equitable adjustment shall be made in the Contract Price or delivery schedule or both in consultation with the Supplier and the Contract shall accordingly be amended. Any claims by the Supplier for adjustment under this clause must be asserted within thirty (30) days from the date of the Supplier's receipt of the Purchaser's change order. If the parties cannot agree on an equitable adjustment, the Change Order will not be implemented.

7.27.3. The parties will agree during development of the Project Plan to a time period prior to the scheduled date for Acceptance, after which all specifications shall be frozen. Any Change Order generated after this time will be dealt with after Acceptance.

7.27.4. The Supplier agrees to design and program additional reports and features to Application Software packages at a price and schedule to be agreed with the Purchaser by means of a Change Order. The compensation for supplier's technical staff responsible for the additional effort shall be computed at mutually agreed rates at the time of requirement.

7.28. EMPLOYEES

During the contract period and for a period of six (6) months thereafter, both the purchaser and the supplier shall refrain from canvassing each other's employees engaged in the performance of the Contract with a view to offering employment.

7.29. TRAINING REQUIREMENTS

The bidder should provide hand holding training to the staff concerned for installation of device and troubleshooting as per para 4.7.9

7.30. TIME FRAME FOR COMPLETION OF PROJECT

PROCUREMENT, INSTALLATION & IMPLEMENTATION OF THE SOLUTIONS

All hardware and software components supplied under the scope must be implemented within the period specified below from the date of issuance of the purchase order. Training to the identified user has to be provided within **2 week** from the date of request from the bank. Integration of devices for collection of logs will be done in a phased manner as per the following details:

I. For Centralized Log Management and Event Correlation

a. Delivery & Installation: All hardware, software and other accessories required for installation - within **8 weeks** from the issuance of purchase order.

b. Phase I
: Integration of all networking and security devices like firewalls, IPSs, Routers, Switches and internet facing servers. This should be completed within - 4 - months of issuance of the purchase order**..**

c. Phase II: All applications and remaining devices integration within - 6- months of issuance of the purchase order.

II. For DAM

a. Delivery & Installation: All hardware, software and other accessories required for installation - within **8 weeks** from the issuance of purchase order

b. Phase I: All critical databases should be integrated with DAM, within -4- months of issuance of the purchase order.

c. Phase II: All other databases within -6- months of issuance of the purchase order.

III. For VM

a. Delivery & Installation: All hardware, software and other accessories required for installation - within **8 weeks** from the issuance of purchase order.

To be made operational within **4 months** from the issuance of purchase order.

7.31. Insurance:
The goods supplied under the Contract shall be fully insured against loss or damage incidental to transportation, storage and erection. The transit insurance shall be for an amount equal to 110 percent of the invoice value of the Goods from "Warehouse to final destination" on "All Risks" basis including War Risks and Strikes. The supplier should also insure the goods in Indian Territory for the invoice value under Storage cum Erection policy till **six** months from the date of delivery. Residual period of insurance policy should be more than 2 months from the date of submission of documents. The supplier has to bear the losses on account of any damage happening to the system due to non availability of storage cum erection policy,

7.32. IT ACT 2000/2008
The Hardware and Software to be quoted as per this tender should comply with the requirements under Information Technology Act 2000/2008 and subsequent amendments

SECTION 8

TECHNICAL SPECIFICATIONS REQUIREMENT

TECHNICAL SPECIFICATIONS REQUIREMENTS

The solution should be able to collect logs at present from 4 sites (3 sites at Chennai and 1 from Hyderabad)
The Bank has DC at Chennai and DR at Hyderabad.
The devices/appliances proposed for the solution at DC & DR must be

- Identical
- Rack mountable with necessary perforated racks(front & Back) and rails.
- Must be in active-passive mode wherever HA/Failover features required in the solution.
- Having hot swappable dual power supply.

Note: In case of customizable, Maximum 2 line items under each Major heading can be permissible for customization in terms of features and not hardware. The customization also should be finished within stipulated timeline of implementation of project as mentioned in RFP. In case if any feature is not readily available & also non customizable, the bid will be liable for rejection.

8.1.SIEM(Centralized Log Management and Event Correlation) Solution Requirements

8.1.1. Physical Appliance Specifications

Sr. No.	Features	Readily Available (Yes/No)	Customizable (Yes/No)
	At Data Centre – Log Management Solution		
1	Log management solution should support at least 5000 EPS and 30,000 net flows with a device support of minimum 500 devices		
2.	The solution should be scalable up to 15000 EPS and 50,000 Netflows and 1000 devices		
3.	The solution Should be available in High Availability-Hot Standby Mode. Auto Failover mode. Please describe the architecture proposed to meet this requirement.		
	At DR Site – Log Management Solution		
1.	Log management solution should support at least 5000 EPS and 30,000 net flows with a device support of minimum 500 devices		
2.	The solution should be scalable up to 15000 EPS and 50,000 Netflows and 1000 devices		
3.	Should be available in High Availability-Hot Standby Mode. Auto Failover mode. Please describe the architecture proposed to meet this requirement.		
	At Data Centre – SIEM Correlation Engine		
1.	The proposed solution should support at least 2500 EPS and 30,000 net flows at correlation layer.		
2.	The solution should be scalable up to 10000 EPS and 50,000 Netflows.		

Sr. No.	Features	Readily Available (Yes/No)	Customizable (Yes/No)
3.	Should be available in High Availability-Hot Standby Mode. Auto Failover Mode.		
4.	Support for the Integration of Security Logs from the following devices/application systems: **Operating System**: Windows 7, Win2K, Win2K3,Win2008, Sun Solaris, Linux,OS/2, HPUX, IBM AIX, different flavors of Unix, Novell Netware, **DataBase Servers :** Oracle, and SQL Servers & Foxpro , Sybase, enscribe **DHCP Server :** DHCPserver supporting Devicesand Operating systems. **Networking Hardware** **Firewall:** Checkpoint , Cisco Pix, Cisco ASA, Juniper **IPS/IDS :** Proventia, Checkpoint **Routers :** Cisco, Juniper **Layer 2 and Layer 3 Switches ;** Cisco, HP, **UTM Devices :** Checkpoint, Cyberoam **Network Behavior Analysis Tools** **VPN Devices** : Cisco, Checkpoint **Virtualization :** VMWare, IBM's LPAR, Citrix, **Microsoft Hypervisor Messaging:** Microsoft Exchange Server, **Web Server :** BEA Web logic, IIS, Apache, Websphere **Customized/Middleware Applications:** Oracle Financials, BEA, Active Directory, Cisco ACS **Antivirus Solutions:** Symantec **Payment Messaging/Transaction Switching system:** Base24, SWIFT, SFMS(Structured Financial Messaging Solution), RBI-INFINET(Indian Financial Network), Cash Management Services This is an indicative list and the product should be capable of integrating the logs for other systems/OS/devices too, which may not be included in the list and may be deployed by the Bank at a later date. (Please provide list of supported platforms/applications/tools)		
5.	The system should be able to integrate with popular tools like Nessus, nCircle, QualysGuard, Foundscan, ISS, Appscan, and other tools as Bank may choose		

Sr. No.	Features	Readily Available (Yes/No)	Customizable (Yes/No)
	to deploy/integrate in future. Please specify name of all VA tools which can be currently integrated.		
6.	Please provide Industry recognition/ award/ certification received by the SIEM solution		

8.1.2. General Architecture and Features

Sr. No.	Features	Readily Available (Yes/No)	Customizable (Yes/No)
1.	The system shall be available in a soft-appliance format or hardware appliance with a hardened OS. The storage configuration must offer a RAID configuration to allow for protection from disk failure.		
2.	The system's architecture shall be scalable and able to expand to larger environments in the future or when requirements grow.		
3.	The system shall compress on-line data as well as offline (archived) data to minimize storage requirements.		
4.	The system shall have a secure and preferably embedded log repository to store logs and shall not require separate database expertise to administer and manage.		
5.	The system shall support archival of collected log information to an external storage medium. Please list all external storage mediums and interface types supported.		
6.	The system shall provide a Monitor page that can display internal statistics such as disk storage used and the current Events Per Second (EPS) flow.		

8.1.3. Centralised Logs Collection and Storage

Sr. No.	Features	Readily Available (Yes/No)	Customizable (Yes/No)
1	There should be a clear physical separation between the collection engine, logging engine and the co-relation engine.		
2	The collector used by the system to collect logs shall be available as a software component/appliance		
3	The system shall support the configuration of the collection of logs from a wide range of network devices, security mechanisms, operating systems and applications across multiple platforms from a single configuration/management console.		

Sr. No.	Features	Readily Available (Yes/No)	Customizable (Yes/No)
4	Information transmitted between the Collector component and event storage solutions must be encrypted. Please describe encryption algorithms used.		
5.	The system shall be able to support caching mode during the transferring of data for collection. The raw events can be stored temporary in log collector if there is network disruption between collector and log storage engine. This is to ensure event data is still being logged in the case of network disconnection, and resume sending of data to log storage engine upon network resume for ensuring zero data loss.		
6.	The system shall support batching of events at the log collector level to improve the throughput by sending multiple events in one network packet. However, should a critical event happen, the collector shall forward it immediately to the log storage engine.		
7.	The system shall provide a software development kit to support standardised application event logging and development of system interface for the collection of logs from in-house or customised applications.		
8.	The system shall be able to capture 100% of the information in the original event data, logs and alert messages and normalize them into a common standard event schema for further analysis, troubleshooting and other data processing needs.		
9	Event storage components must authenticate event transmissions and not accept event data from unauthenticated sources.		
10	The system shall support normalization of the logs so that there is a common schema across all device sources.		
11	The system shall support categorization by providing intuitive categorization taxonomy so as to ensure that the end users do not have to know or understand the source devices specific event terminology / syntax.		
12	The system shall allow bandwidth management i.e. rate limiting at the log collector level so as to minimize disruption to the Enterprise's network bandwidth utilization and availability.		
13	The system shall be able to integrate new data sources into existing collectors, without disruption to the ongoing data collection.		
14	The system shall support aggregation technologies that consolidate multiple identical raw events into one processed event.		

Sr. No.	Features	Readily Available (Yes/No)	Customizable (Yes/No)
15	The system shall support filtering technologies where unwanted logs can be filtered away at the log collection layer.		
16	Event transport must use compression technologies to reduce overall bandwidth required to transmit event data between collection components and event storage solutions. Please specify compression used and average compression reduction achieved during event transport.		
17	Event transport must be able to send to multiple destinations for HA / DR purposes. Each transport path must be independently configurable from the other.		
18.	Stored events must be able to have their integrity validated using FIPS 140-2 approved integrity hashing algorithms. Please state the algorithms used for each component that stores log events.		
19.	Event data must be enhanced in a manner that allows all content developed (filters, dashboard displays, reports) to be vendor agnostic (i.e.: a currently deployed technology can be replaced with a similar technology without having to modify existing content on the log management or SEIM solution).		
20.	The system shall provide custom-defined fields that allow for insertion of additional data into the event based on user-defined parameters.		
21.	All fields in the event must be available for filtering, displaying, reporting and use in correlation conditions.		
22.	The encryption algorithms and protocols used shall be widely accepted in security community and not proprietary in nature. Please state the encryption algorithms and protocols used.		
23.	The system shall provide configurable transfer of logs in real time and batch transfer modes.		
24.	The system shall provide a Syslog collection capability that listens for logs records sent directly via Syslog over UDP and TCP		
25.	The system shall provide a file-based collection capability to collect raw files from remote systems via FTP, SCP or SFTP.		
26.	The system shall be capable of supporting common log delivery methods. These shall include e.g. Syslog, OPSEC, SDEE, SNMP, raw text files, ODBC/JDBC and XML files.		

Sr. No.	Features	Readily Available (Yes/No)	Customizable (Yes/No)
27.	The system shall provide a remote file-based collection capability to collect raw files located on a NFS storage or Windows file servers via CIFS.		
28.	The system shall be able to protect the privacy of users by having the ability to mask certain fields or event information		
29.	The solution should have the capability to compress the logs to by at least 70% for storage optimization. Documentary support should be provided.		
30.	Data Archival solution should store information in tamper proof format and should comply with all the relevant regulations.		
31.	RAW logs that are received by the Collector/Agent/Logger/SIEM solution should be Authenticated and compressed before being written to storage. Also data integrity checks must be enforced to ensure that the logs are tamper proof.		
32.	The SIEM Solution Database should write logs in tamper proof manner. Once the logs are written to the disk/database no one including SIEM or database/system administrator should be able to modify/tamper/delete the stored logs till archival of the same		

8.1.4. Logging and Searching Capabilities

Sr. No.	Features	Readily Available (Yes/No)	Customizable (Yes/No)
1	The system shall have the capability to allow users to perform structured AND unstructured queries against log information. Describe query languages or syntax used by the system.		
2	The system shall have the function to add indexes to both structured AND unstructured data to enhance searching performance.		
3	The system shall be able to perform distributed searching. For example, the user could search for the action “Failed Login” and this search query will be executed automatically on all the deployed systems and the results returned back to the user on the same screen.		

Sr. No.	Features	Readily Available (Yes/No)	Customizable (Yes/No)
4	The system shall allow such queries to be saved and have the capability to allow such queries to be re-loaded in the future.		
5.	The system shall allow different devices to be categorized together into the same group. For example, ten different Windows servers can be categorized into the "Production" server group. The user could then search for this "Production" server group without manually specifying the IP addresses for these ten Windows servers.		

8.1.5 Incident Analysis and Response

Sr. No.	Features	Readily Available	Customizable
1.	The system shall provide attack information and the corresponding security impact of the attack. In order to derive an accurate impact of the attack, the system shall take into consideration the Model Confidence (i.e. how well do we know the target), the Severity (what is the history of the attacker and the victim), the Relevance (how vulnerable is the target) and Asset Criticality (how important is the asset). A priority value shall be given based on the above.		
2.	The system shall support ease of use by offering unlimited drill down capability down to the capture event data, logs or alert message from the detected incident or threat.		
3.	The system shall support dashboards or widgets that are made up of individual data monitors in a variety of graphical and tabular formats. These dashboards shall be use to summarize the event flow and communicate the effect of event traffic on specific systems on the network.		
4.	The system shall allow the analyst to specify a "watch list" to monitor and keep track of events of interest e.g. event types, IP addresses etc.		
5.	The events of interest tracked and monitored by the "watch list" must be updated in real time as the system receives the event data, logs and alert messages.		
6.	The events can be displayed based on user preferences and display templates can be sorted easily based on majority fields such as event priority, event start time, end time, attacker IP, target IP, etc.		

7.	The system shall support multiple active events views displayed in the manager based on customized display templates.		
8.	The system shall provide a wide array of filtering options that can be applied to all fields in the captured events Please list the filtering options.		
9.	Filtering options shall support Boolean. Kindly list the Boolean operations."		
10.	The system shall provide a dynamic graphical representation of the event relationship in the real time, and group similar and/or related events with identical fields and show the count at the console.		
11	The system shall provide a user friendly graphical user interface to create/edit/delete correlation rules without any scripting/programming involvement.		

8.1.6. Real Time Aggregation, Normalisation and Correlation of Collected Logs

Sr. No.	Features	Readily Available (Yes/No)	Customizable (Yes/No)
1.	The system should have the capability to monitor privilege users of different systems. Also Database monitoring for access and configuration changes should be possible.		
2.	The system shall provide out of box pre-defined correlation rules for commonly known attacks.		
3.	The system shall support the ability of having rules executing programs whenever rules are fired. It shall have the flexibility of passing variables such as IP address, network ports etc. to the programs that are being executed.		
4.	The system must be able to detect multi-stage attack where the multi-stage attack can be detected using correlation to join events spanning a session over time. The system must combine and relate values from multiple events, such as from an IDS and a firewall, to infer that the attack was perpetrated.		
5.	The system must demonstrate how the product can define unique correlation content based on the organization's specific and unique policies. Examples of such policies are: 1. Ensuring proper audit logging is set for devices and applications 2. Alerting when Flash Drives are used, or when confidential information is copied to them		

Sr. No.	Features	Readily Available (Yes/No)	Customizable (Yes/No)
6.	The system shall be able to replay historical events for analysis whenever required.		
7.	The system shall have capability to add asset information including physical location, asset description, IP address, asset ownership, contact information, role of the server with regards to the business function etc.		
8.	The system shall support defining the event priority based on the asset criticality input by system owner.		
9.	The system shall correlate the event using the asset information or based on number of occurrence of specific events as part of the condition definition and filter to trigger an automated escalation process for response and remediation.		
10.	The system shall have the capability to automatically represent detected attacks in graphical view.		
11.	The system shall be able to display real-time trend data of filtered events at the correlation manager.		
12.	The system shall be able to group data of similar contents with certain identical fields and show the count at the correlation manager.		
13.	The system shall provide a customizable view of data selectable from graphs, maps, charts and graphics.		
14.	The system shall allow selection of events with desired parameters or based on any selection fields in the events.		
15.	The system shall provide the ability to display “whois” information based on IP address		
16.	The system shall provide additional geographical information such as the Country based on IP address and demonstrate how the product can correlate information based on the global location of the event’s subjects.		
17.	The system must be able to demonstrate correlation of events based on asset vulnerability data. The vulnerability scan data and the IDS/AV data must not have to come from the same vendor.		
18.	Physical vs. Logical Correlation: The system must demonstrate how the product can correlate information based on physical locations and logical actions.		

Sr. No.	Features	Readily Available (Yes/No)	Customizable (Yes/No)
19.	Business Relevance Correlation: Bidder **must** demonstrate how the product can correlate and prioritize events based on relevance and mission criticality of the organization's assets **in case bank decides**.		
20.	The solution **should** dynamically learn behavioral norms and expose changes as they occur. Detail the methods used by the solution and the method by which anomalies are displayed.		
21.	The solution **should able to** detect denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks. Describe how the solution detects and displays this information.		
22.	The solution **should** detect and present views of traffic pertaining to observed threats in the network. Describe the types of threats and visualizations for this information in the Security Intelligence system.		
23.	The solution **should** identify network traffic from potentially risky applications (e.g. file sharing, peer-to-peer, etc.). Please describe how your solution meets this requirement.		
24.	The solution **should** able to automatically change the credibility weightings of security devices in response to network-wide attacks. Please describe how your solution meets this requirement.		

8.1.7. Performance and capacity

Sr. No.	Features	Readily Available (Yes/No)	Customizable (Yes/No)
1	The system shall support multi-hierarchy mode where you can stack multiple correlation engines together to give you greater performance.		
2	The system shall present the processed data at the correlation manager display within few seconds from the time of the data reaching the manager.		
3.	The system shall be able to allow the user to retrieve the system logs for diagnostic purposes or to send such logs to the company's Support department for troubleshooting.		

Sr. No.	Features	Readily Available (Yes/No)	Customizable (Yes/No)
4	The system shall have the capability to automate purging of log information after a defined period of time.		
5	The system shall allow data retention policies to be changed easily after the initial setup.		
6	The system shall alert the administrator on system alerts such as low storage space.		
7	The system shall have the capability to assign specific permissions to perform actions for management and analysis of stored log information.		
8	The system shall have the capability to configure certificate-based encryption to secure transmission of events.		
9	The system shall have the capability to authenticate users from an external directory such as RADIUS.		
10	The system shall have a overall view of the tasks that have been scheduled. An example of a scheduled task could be a Daily Report on Failed Logins. Such overall view will allow the user to have a visibility on the number of background tasks running on the system.		

8.1.8. User Access Control and General Administration

Sr. No.	Features	Readily Available (Yes/No)	Customizable (Yes/No)
1.	The system shall provide the function to update the product version or components such as reports packages. This process shall occur seamlessly and transparently		
2.	The system shall log all key actions for auditing purposes		
3.	The system shall support role based access control for different user groups to access different devices information, views, filters, templates.		
4.	The system shall provide a secure web access for different user groups to access reports and resources.		
5.	The system shall provide access controls to allow administrator to define the reports and resources accessible by each user group.		

Sr. No.	Features	Readily Available (Yes/No)	Customizable (Yes/No)
6.	The system is able to authenticate directly through Active Directory or LDAP for user log in.		
7.	The system must be able to generate audit trail for all activities done by users or processes on the system		
8.	The system shall be able to report on its own system health and availability. Notifications shall be sent out if the system health or availability is failing		
9.	The system shall provide a management utility with automated scheduled archiving functionality for the archival of online and offline data based on the data retention policy		
10	The system solution shall support the configurable data retention policy.		
11	The system shall support centrally controlled agents/log-collectors upgrade		

8.1.9 Reporting and Alerting

Sr. No.	Features	Readily Available (Yes/No)	Customizable (Yes/No)
1.	The system shall provide the functionality to export the report in the following format: • PDF • CSV • HTML • Flat file format		
2.	The system shall provide a report designer that allows users to customize the appearance of the report such as adding of organization logo in the report, modifying the graphs, tables, grouping, sorting, etc.		
3.	The system shall provide real-time or near real-time alerts for detected incidents		
4.	The system shall integrate with SMS gateways and email systems to deliver the alerts to the analysts.		

Sr. No.	Features	Readily Available (Yes/No)	Customizable (Yes/No)
5.	The system shall allow the analyst to define criticality level of the incident and the corresponding mode of alert		
6.	The system shall have the ability to schedule reports for generation.		
7.	The system shall provide the functionality for the generation of the reports based on assets, incidents, threats, impact, "watch-list", or any other event fields.		
8.	The system shall provide the ability to trigger configurable email messages based on specific rules.		
9.	The system shall allow ownership of end devices be defined so that alerts are sent to individuals responsible for those devices.		
10	The system should able to generate authoritative/compliance reports based on standards from governing bodies for ISO/IEC and PCI Security Standards Council. The solution should have option to customize reports based on any government regulation e.g RBI standard/guidelines.		

8.1.10. Workflow Management

Sr. No.	Features	Readily Available (Yes/No)	Customizable (Yes/No)
1.	The system shall have built-in case management that allow user to create/update case upon receiving of events for escalating to the correct support areas as part of the incident handling management process		
2.	The system shall have a structure or Stages that defines the steps of the event annotation or case management workflow and the users and user groups that can be notified.		
3.	The workflow management functionality shall enable the analysts to assign opened cases to respective users/roles.		

Sr. No.	Features	Readily Available (Yes/No)	Customizable (Yes/No)
4.	Solution must be able to export event information through both automated (as a result of a correlation action) or manual (as a result of an end-user action) methods in a manner suitable for processing by third-party tools.		
5.	Solution must be able to integrate with third-party Help Desk systems such as BMC Remedy/ca/IBM/HP etc. Integration must support at a minimum: automated and manual incident creation, updating of existing incident, synchronization of incident closure		
6.	Solution must be able to interface with third-party forensic investigation tools such as EnCase, NetWitness, NikSun through seamless user actions. Please list successfully deployed integrations.		
7.	Solution should be capable of supporting integration into existing organizational knowledgebase websites that contain processes, procedures and other information related to the analyst's job function.		
8.	The system shall allow the assigned officer to update the progress of the incident investigation and add comments to the assigned cases		
9.	The system shall provide a dashboard to allow the analysts to keep track and monitor the progress of the incident investigation assigned to the respective officers.		
10	The system shall allow the officer to close the cases upon conclusion of the investigation of the incident.		
11.	The system shall provide an automatic notification escalation for notifications which did not receive an acknowledgment during a specified time-frame.		
12	The system shall provide the ability to support file attachments to specified cases that has been created.		

8.1.11. Storage & Backup/Recovery

Sr. No.	Features	Readily Available (Yes/No)	Customizable (Yes/No)
1.	**Storage for SIEM** – 20 TB on RAID 5 at Data Centre & 20 TB on RAID 5 at DR Site (appliance itself or attached SAN). Appliance should not contain DAS. The Storage should be scalable to 50 TB. It should store both raw log as well as normalized logs.		
2.	The Storage system must have at least two controllers with failover to each other or to a separate standby controller in case of any of the running controller failure.		
3.	The storage shall have an ability to protect the data in cache if a storage or controller fails due to some reason like power failure, physical failure etc. The storage array must have complete cache protection mechanism.		
4.	The system shall have backup functions available in case of hardware failure. The backup should contain the system configuration such as IP address, users/groups and reports.		
5.	The system shall be able to work in a redundancy fashion by e.g. purchasing another similar model and by configuring the log sources to send to these two systems simultaneously.		
6.	The system shall be able to recover all its settings if a backup file is available. For example, if there is a hardware failure and a new replacement system has been delivered, the user can recover the system with all the settings before the failure by deploying the latest backup file.		
7.	The system should have support for the mix of 600GB or higher SAS (15K RPM and 10K RPM) & 1000GB or higher SATA-II (7.2K RPM) disk drives on the same controller/storage array.		
8.	The configuration must be proposed with a RAID based solution to protect against simultaneous dual-disk failures in the same RAID group with an ability to expand the RAID group online by addition of disk drives. The no. of disks in the RAID group should be configured as per the storage best practices.		

Sr. No.	Features	Readily Available (Yes/No)	Customizable (Yes/No)
9.	It should be configured with at least 20 TB of usable space using 600GB SAS 10K RPM disk drives, and should scale to 50 TB usable on the same type of HDD's. This capacity should exclude all the overheads involved like RAID overhead, Storage OS, Spare disks.		
10	The storage system must have at least 2 x 8Gbps FC ports per controller for host/switch/tape connectivity		
11	The storage system must be configured to hold snapshots per volume/LUN without any performance degradation.		
12	The proposed solution should be configured with Data Replication feature and necessary hardware for FC-IP conversion if required should also be configured.		
13	Replication S/w should support SAN data and should also support both sync and async modes.		
14	Replication Licensing should support the maximum capacity of the storage quoted.		
15	System should have capacity to maintain the logs for **1 year** online and other logs should be archived		
16	System should provide the backup facility for data, configuration and whole system on secondary storage such as LTO tapes.		
17	**Backup & Offline Storage** – Rack Mountable autoloader Tape Library		
18	Rack Mountable Tape Library with minimum 2 LTO 5 FC drives and data protection capability. It should have minimum 24 LTO Cartridge slots.		
19	The Library should have an integrated Bar Code reader and vendor to supply 150 nos. of bar code labels.		
20	The Tape Library should be able to scale up in terms of no. of Slots as well as No. of Drives by stacking additional modules in pass thru mode.		

Sr. No.	Features	Readily Available (Yes/No)	Customizable (Yes/No)
21	The Tape library should have Redundant hot swappable power supply		

8.2. DATABASE ACTIVITY MONITORING TOOL

Sr. No.	Features	Readily Available (Yes/No)	Customizable (Yes/No)
1.	Solution can be either software based or appliance based. In case of software based solution, please mention the hardware configuration being offered. It should able to handle atleast 150 transaction per second and should cater more than **100** databases.		
2.	Solution should be able to receive feeds from a mirrored port as well as from the agents installed on the database servers.		
3.	For monitoring DBA activities, an agent should be deployed on database servers and there should be only one agent for monitoring DB activities including local DB local DB traffic and the network DB traffic.		
4.	Agents should have only minimal overhead for the production DB servers. The CPU utilization on the DB server should not increase beyond 5% other than present utilization.		
5.	Agent should support different versions of Windows, Unix, AIX Linux and their different flavors. Please provide a list of all the supported platforms and their flavors.		
6.	Audit trail should be stored within the solution in secured and tamperproof manner.		
7.	Solution components (Agents and manager should be managed centrally.		
8.	Solution should support below DB platforms, their different flavors and versions • *Oracle* • *MS-SQL Server* • *Sybase* • Base24 • Please provide a list of all the supported Databases and their flavors		

Sr. No.	Features	Readily Available (Yes/No)	Customizable (Yes/No)
9.	Solution detect sensitive data types, such as credit card numbers etc, in database objects.		
10.	Solution should have Database vulnerability assessment tests for assessing the vulnerabilities and mis-configurations of database servers, and their OS platforms. Oss and RDBMSs are tested for known exploits and mis-configurations. The product should identify missing patches.		
11.	The product should have pre- defined reports and support custom report generation. Please provide list of reports readily available.		
12.	The solution should offer virtual patching capabilities (protecting the database from known vulnerabilities without deploying a patch or script on the system).		
13.	The solution should support high availability		
14.	The product should be able to be installed in sniffing (promiscuous) mode or inline mode.		
15.	Solution should have built-in bypass for inline mode.		
16.	The solution should not use the native database auditing functionality.		
17.	Solution should be able to integrate with the SIEM solution, Dashboard and Incident Management solution being proposed by the vendor.		
18.	The data transferred between the agent and the appliance should be through an encrypted *channel.*		
19.	The solution should capture at least the following activity by user/role - *Update, insert, delete(DML)* - *Schema/Object changes* (DDL) - Manipulation of accounts, roles and privileges (DCL) - Backend SQL query updates.		
20.	Please provide Industry recognition/ award/ certification received by the DAM tool		

8.3. VULNERABILITY MANAGEMENT TOOL

Sr. No.	Features	Readily Available (Yes/No)	Customizable (Yes/No)
1.	Solution should at minimum support assessments of all the platforms in the DC and DR environment of the bank. Please provide list of supported platforms. The VM solution should include both hardware and application. It should handle atleast 100 IPs.		
2.	The application should be web based which can be installed centrally and accessed by users across organization in different offices.		
3.	The application should have comprehensive predefined security configuration assessment checks (setting) for different supported platforms as per industry standards such as ISO27001, PCI-DSS, OWASP etc.		
4.	The application should have all security configuration setting checks recommended by CIS for the supported platforms.		
5.	The application should allow organizations to create multiple assessment profiles for any supported platform.		
6.	The application should allow organizations to create different profiles as per their organization requirements.		
7.	The application should allow organizations to customize the checks as per the organization policy and requirements.		
8.	The application should provide Secure Configuration Document for all the platforms. These SCDs should have crisp step-by- step implementation (How-to configure) steps for all checks		
9.	The application should allow organizations to create asset details of all servers and devices with their IP, platform details, owner, location, department and value of the asset.		
10.	The application should allow organizations to manage asset details.		
11.	The application should allow organizations to choose an assessment profile at asset level.		

Sr. No.	Features	Readily Available (Yes/No)	Customizable (Yes/No)
12.	The application should allow search of assets based on IP, Location, Owner and Department.		
13.	The application should support multiple approaches for vulnerability assessment,		
14.	The application should perform the vulnerability assessment remotely over the network without any manual intervention.		
15.	The application should not require any of their agents to be pre-installed in the target assets to enable automated VA.		
16.	The application should allow organizations to schedule the VA of selected assets for a pre-defined date and time.		
17.	The application should allow organization to know the status of the scheduled automated VAs. In case of issues, the application should provide appropriate information at asset level and check level.		
18.	The application should provide scripts or light-weight executables to manually collect the security configuration data from the assets.		
19.	The application should support upload of the security configuration data for detailed assessment and analysis.		
20.	The application should provide option to raise exceptions for unsafe checks at asset level with appropriate reason.		
21.	The application should maintain these exceptions at asset level till such time the exceptions are flagged off.		
22.	The application should report the exceptions accordingly in VA Reports.		
23.	The application should generate reports and analysis a. Summary Report of assets scheduled for VA b. VA Report 🕐 Asset Level Report with Analysis 🕐 Asset Level Report with safe and unsafe values c. Trend Reports 🕐 Vulnerability Status of an Asset over multiple VA Cycles 🕐 Vulnerability Summary over multiple VA Cycles		

Sr. No.	Features	Readily Available (Yes/No)	Customizable (Yes/No)
24.	The application should allow export of reports to different formats such as PDF, MS- EXCEL etc.		
25.	The application should have a Dashboard which shows important statistics including, Vulnerability Assessment status, Trend of VA outcome over the period, Assets pending VA for longer period of time, etc.		
26.	The application should support users to be created and authenticated in the application		
27.	The application should allow the organization hierarchy to be defined with multiple levels		
28.	The application should control the privilege to manage assets, ability to create reports and access to reports and analysis based on privileges assigned and based on hierarchical level of the user		
29.	The application should have strong application security controls such as, a. Password and account policy b. Assignment of privileges to users/roles at granular level c. Detailed Audit trails		
30.	Application should support broad range of systems, their different versions, flavors, vendor products Make and models such as Operating Systems Network and security devices Standard applications such as Web servers, Mail Server etc Please provide list of such supported systems.		
31.	Please provide Industry recognition/ award/ certification received by the VM tool		
32.	Does the proposed solution support risk-based scoring metrics ?		
33.	Proposed solution should perform Intelligent port scanning for service identification running on non-standard ports and also support scanning throttling/ rate limiting speed.		
34.	Solution should be capable of Policy Compliance, Baseline Policy Scan		

Sr. No.	Features	Readily Available (Yes/No)	Customizable (Yes/No)
35.	Proposed solution should have ability to control multiple scanning instances from a centralized location/console		
36.	Scanning engines should support parallel scan windows to increase the scan speed		
37.	Proposed solution should have configurable performance options to avoid target device/network saturation. Please provide details.		
38.	Proposed solution should have ability to search vulnerability check database by vulnerability name, CVE, patch #/name, /advisory #, bulletin #, category (e.g. OS, database, web, etc…)		
39.	Proposed solution should have the ability to include/exclude specific vulnerability checks into a scanning policy		
40.	Proposed solution should have granular control over what ports are included in the port scan		
41.	Proposed solution should provide a network topology map to have high level overview		
42.	Proposed solution should support following discovery options - ICMP, DNS lookup, TCP port ping, UDP port ping		
43.	Proposed solution should be able to integrate with SIEM, Incident management and Dashboard solutions- Please provide list of such solutions		
44.	Proposed solution should support correlation of new threats / Vulnerabilities with the existing infrastructure		
45.	Proposed solution should provide an executive dashboard to give overall security posture of the network / systems		
46.	Proposed solution should generate scanned reports in HTML, PDF, XML and CSV formats		
47.	Proposed solution should support compliance report generation for PCI DSS, OWASP, Basel II, ISO 27001, SANS Top 20, COSO / COBIT		
48.	Proposed solution should have the ability to generate custom reports		

Sr. No.	Features	Readily Available (Yes/No)	Customizable (Yes/No)
49.	Proposed solution should have ability to search current and historical data By IP, Hostname, Network or Vulnerability		
50.	Report generated by Proposed solution should display both open and closed vulnerabilities		
51.	Proposed solution should generate reports based on hosts, networks, geographies or departments / business units		
52.	Proposed solution should generate report to view total # of vulnerabilities over time period including specific ones like - only high or medium or low		
53.	Proposed solution should generate following reports		
54.	Types and # of systems: Host breakdown by OS (both % and #)		
55.	Can this be further broken down into workstations, servers, and network devices?		
56.	Vulnerabilities found by criticality (critical, high, medium, low)		
57.	Top X vulnerabilities (by occurrence)		
58.	Top X critical/high vulnerabilities (by occurrence)		
59.	Average vulnerabilities per system (workstation, server, network device); Alternatively could be risk rating per system		
60.	Top X most vulnerable systems		
61.	Proposed solution should produce an asset-centric report, i.e. according to how business units are organized, rather than scan-centric or network-centric reports		
62.	Proposed solution should have the ability to generate custom reports.		

SECTION 9

BID FORM, PRICE SCHEDULES AND OTHER FORMATS

9.1. TECHNICAL BID

TO Date:
INDIAN BANK
Corporate Office
Chennai 600 014

Dear sir,

Sub: **Implementation of a Comprehensive Log Management, Event Correlation, Database Activity Monitoring & Vulnerability Management Solutions**

Having examined the Bidding Documents including Addenda Nos. .....(insert numbers),the receipt of which is hereby duly acknowledged, we, the undersigned, offer to provide **Implementation of a Comprehensive Log Management, Event Correlation, Database Activity Monitoring & Vulnerability Management Solutions** and submit our technical Bid as follows:

The specifications for the following areas as per your scope of work are duly filled in by us along with our comments wherever required and they are enclosed along with this.

List of deviations from the required specifications:

1)
2)
(If left blank, it is treated that there are no deviations in the compliance of specifications)

We offer a warranty period of **One Year** from the date of installation of the equipment and other solutions or 18 months after the date of receipt of shipment at the destination, if the installation is delayed due to Bank, whichever period concludes earlier. The warranty will be as per Scope of work under your bid document.

We agree for insuring the systems during transit and covering of storage cum erection risk for a period of **six** months from the date of delivery at the destination. Residual period of insurance policy should be more than 2 months from the date of submission of documents

We enclose the technical brochures for the models quoted.

We submit that we should abide by your terms and conditions governing the quotations and Warranty mentioned in the bidding document.

We submit that we abide by the details given above.
We undertake, if our bid is accepted, to complete the services in accordance with the delivery schedule specified in the bid.
We undertake to execute Service Level Agreement (SLA), Non Disclosure Agreement (NDA) and other forms for this tender as per Bank's format.
If our bid is accepted, we will obtain the guarantee of a bank in a sum equivalent to 10% of the contract amount for the due performance of the Contract, in the form prescribed by the Bank.

We agree to abide by this for the bid validity period specified and it should remain binding upon us and will be accepted at any time before the expiration of that period.

Until a formal contract is prepared and executed, this bid, together with your notification of award, should constitute a binding Contract between us.

We undertake that, in competing for (and, if the award is made to us, in executing) the above contract, we will strictly observe the laws against fraud and corruption in force in India.

We understand that you are not bound to accept the lowest or any bid you may receive.

We clarify/confirm that we comply with the qualification criteria of the bidding documents.

Dated this..... Day of..... 20.....

.....
Signature

(In the Capacity of)

..... Duly authorised to sign bid for and on behalf of (give below the Name & Address of Bidder) – Please enclose authorization letter from the competent authority authorizing the signatory to sign the documents.

Note:

The Technical Bid shall include the following:

1. Detailed Project Plan corresponding to the deliverables as required by INDIAN Bank for the project.
2. The Project Plan should indicate the milestones and time frame of completion of the activities of the Project.
3. The solution provider is required to give details of standards followed
4. Resources and support required from the Bank to be defined clearly
5. The solution should cover all the requirements specified in the General Requirements of the solution.
6. The data available within the system/networks should not be exported outside the network and should not be stored in any systems other than the one assigned for such storage.
7. The solution provider should give an undertaking on the above points.

9.2. MANUFACTURER'S AUTHORIZATION FORM

No. _____ dated

To

Dear Sir:

BID REF. NO. HO/TMD/ ISS/PG/379 /2012-13 dated 05.09.2012

We _____ who are established and reputable manufacturers of _____ *(name & descriptions of goods offered)* do hereby authorize M/s _____ *(Name and address of bidder)* to submit a bid, and sign the contract with you for the goods manufactured by us against the above bid.

We hereby extend our full warranty as per Conditions of Contract for the goods and services offered for supply by the above firm against this bid.

We would provide support/upgrade during contract period, in case the bidder is not able to provide the same.

We confirm that the hardware/software mentioned in Technical bid by bidder to support their solution meets the requirements of the tender.

Yours faithfully,

(Name)
(Name of manufacturers)

Note: This letter of authority should be on the letterhead of the manufacturer and should be signed by a person competent and having the power of attorney to bind the manufacturer. The Bidder should include it in their bid.

9.3. BIDDER PROFILE

General				
Company Name				
Name of the CEO				
Date of Incorporation				
Date of Commencement of business				
Name of the Principal Banker and address				
Holding Company or Parent Company (if any), If holding Company, Name of the parent company				
Company's Head Office: Address Phone : Fax : E-Mail : Chennai Office, If any:				
Details of Service support Centres in Chennai, Hyderabad				
Please provide details of ownership: private/public; Holding company, If any. Top 3 shareholders				
Number of years of experience in	Deployment of the proposed solutions			
	Establishing and Managing Security Operations Center (SOC)			
Name of the Contact person/s				
Phone / Mobile/ FAX number/s				
Financial Background for last 3 Years (in Crores)		1st year	2nd Year	3rd Year
Turnover				
Net Profit After TAX				
Total Assets				

Total Liabilities			
Staff			
	In the company		
Total number of employees			
Administrative staff Technical staff involved in • Management of the proposed solutions (Solution-wise) • SOC Operations Field Engineers			
Solutions Partnership			
Others			
List of Deliverables as per the Scope of Work/General Requirements of the Solution			
Is Company ISO Certified? If yes, provide information along with true copy of the certificate			

9.4. CLIENTS' REFERENCE FORMAT

Similar Projects carried out in India

The following information should be provided in the format below separately for each PROJECT for which the client legally contracted your Company. (Please attach additional sheets wherever necessary)

Name of the client		
Total Value of the project given to the Company		
Contact person from the client side for reference purpose on details of this project		
Contact Phone Nos. of the Client		
Name and Nature of the Project	Deployment of Log Management And Event Correlation	
	Deployment of DAM	
	Deployment of VM	
	SOC Management	
Names of the implemented solutions with their brand		
When the project was executed: Start Date : Completed Date :		
Duration of the project		
Any other relevant details on the project like No of EPS managed, number of devices being managed, services being offered, total time to commission of project (module wise), SOCs established & maintained, etc.		

9.5. BID SECURITY FORM

Whereas .....*(hereinafter called "the Bidder")* has submitted its bid dated ..... *(date of submission of bid)* for the supply of/providing services for ..... *(name and/or description of the goods/services)* (hereinafter called "the Bid").

Know all people by these presents that We ..... *(name of bank)* of ..... (name of country), having our registered office at ..... *(address of bank)* (hereinafter called "the Bank"), are bound unto Indian Bank in the sum of _____for which payment well and truly to be made to the said Bank, the Bank binds itself, its successors, and assigns by these presents. Sealed with the Common Seal of the said Bank this ____ day of _____ 2012____.

THE CONDITIONS of this obligation are:

1. If the Bidder

(a) withdraws its Bid during the period of bid validity specified by the Bidder on the Bid Form; or

(b) does not accept the correction of errors in accordance with the Instructions to Bidders; or

2. If the Bidder, having been notified of the acceptance of its bid by the Bank during the period of bid validity:

(a) fails or refuses to execute the Contract Form if required; or

(b) fails or refuses to furnish the performance security, in accordance with the Instruction to Bidders.

We undertake to pay the Bank up to the above amount upon receipt of its first written demand, without the Bank having to substantiate its demand, provided that in its demand the Bank will note that the amount claimed by it is due to it, owing to the occurrence of one or both of the two conditions, specifying the occurred condition or conditions.

This guarantee will remain in force up to and including sixty (60) days after the period of the bid validity, and any demand in respect thereof should reach the Bank not later than the above date.

.....
(Signature of the Bank)

NOTE : 1. The bidder should ensure that the seal and CODE No. of the signatory is put by the bankers, before submission of the bank guarantee.
2. Bank guarantee issued by banks located in India should be on a Non-Judicial Stamp Paper of requisite value.

9.6. CONTRACT FORM

THIS AGREEMENT made the .....day of....., 2012... Between INDIAN Bank (hereinafter "the Purchaser") of the one part and..... *(Name of Supplier)* of..... *(City and Country of Supplier)* (hereinafter called "the Supplier") of the other part :

WHEREAS the Purchaser invited bids for certain Goods and ancillary services viz., ... *(Brief Description of Goods and Services)* and has accepted a bid by the Supplier for the supply of those goods and services in the sum of ..... *(Contract Price in Words and Figures)* (hereinafter called "the Contract Price").

NOW THIS AGREEMENT WITNESSETH AS FOLLOWS:

1. In this Agreement words and expressions shall have the same meanings as are respectively assigned to them in the Conditions of Contract referred to.

2. The following documents shall be deemed to form and be read and construed as part of this Agreement, viz.:
   (a) the Bid Form and the Price Schedule submitted by the Bidder;
   (b) the Schedule of Requirements;
   (c) the Technical Specifications;
   (d) the Conditions of Contract;
   (e) the Purchaser's Notification of Award.

3. In consideration of the payments to be made by the Purchaser to the Supplier as hereinafter mentioned, the Supplier hereby covenants with the Purchaser to provide the goods and services and to remedy defects therein in conformity in all respects with the provisions of the Contract.

3. The Purchaser hereby covenants to pay the Supplier in consideration of the provision of the goods and services and the remedying of defects therein, the Contract Price or such other sum as may become payable under the provisions of the Contract at the times and in the manner prescribed by the Contract.

Brief particulars of the goods and services which shall be supplied/provided by the Supplier are as under:

SL. NO.	BRIEF DESCRIPTION OF GOODS & SERVICES	QUANTITY TO BE SUPPLIED	UNIT PRICE	TOTAL PRICE

TOTAL VALUE:
DELIVERY SCHEDULE:

IN WITNESS whereof the parties hereto have caused this Agreement to be executed in accordance with their respective laws the day and year first above written.

Signed, Sealed and Delivered by the
said ..... (For Indian Bank)
in the presence of:.....
Signed, Sealed and Delivered by the
said ..... (For the Supplier)
in the presence of:.....

9.7. PERFORMANCE SECURITY FORM

Bank Guarantee No. Date :

To : INDIAN BANK :

WHEREAS ..... (Name of Supplier) hereinafter called "the Supplier") has undertaken , in pursuance of Contract No..... dated,..... 2012 to supply..... .....(Description of Goods and Services) (hereinafter called "the Contract").

AND WHEREAS it has been stipulated by you in the said Contract that the Supplier shall furnish you with a Bank Guarantee by a recognized bank for the sum specified therein as security for compliance with the Supplier's performance obligations in accordance with the Contract.

AND WHEREAS we have agreed to give the Supplier a Guarantee:

THEREFORE WE hereby affirm that we are Guarantors and responsible to you, on behalf of the Supplier, up to a total of .... (Amount of the Guarantee in Words and Figures) and we undertake to pay you, upon your first written demand declaring the Supplier to be in default under the Contract and without cavil or argument, any sum or sums within the limit of ..... (Amount of Guarantee) as aforesaid, without your needing to prove or to show grounds or reasons for your demand or the sum specified therein.

This guarantee is valid until the .....day of.....

Signature and Seal of Guarantors

.....

Date.....2012.....

Address:.....

.....

NOTE :

1. Supplier should ensure that seal and code no. of the signatory is put by the bankers, before submission of the bank guarantees.
2. Bank guarantees issued by banks located in India shall be on a Non-Judicial Stamp Paper of requisite value

9.8. COMMERCIAL BID (To be submitted after completion of **Online Reverse Auction)**

TO Date:

INDIAN Bank
Corporate Office,
Technology Management Department
Chennai-600014

Dear sir,

Sub**: Implementation of a Comprehensive Log Management, Event Correlation, Database Activity Monitoring & Vulnerability Management Solutions**

Ref: Your bid document No: TMD/ISS/PG/379/2012-13 Dated 05.09.2012
Online Reverse auction dated: _____.

Further to the online reverse auction dated _____, we give below the breakup details.

PRICE SCHEDULE (Amount in Rupees)
Note : Below Line Items should meet all requirements as per Technical Specification Additional line items are mentioned in OTHERS column. Onsite L2 Engineer should be part of the overall solution as mentioned in RFP.

PART A – Details as per Section 8 of RFP

SL NO	Description	High Availability Required	(A) CAPITAL COST (inclusive of all taxes)	(B) AMC Cost for 2nd, 3rd, 4th & 5th year (Exclusive of Service Tax)	
			Software , Hardware.	Per Quarter	Total (for 16 Quarters)
1	Centralized Log Management (DC)	Yes			
	Centralized Event Correlation(DC)	Yes			
2	Centralized Log Management (DR)	Yes			
	Centralized Event	No			

SL NO	Description	High Availability Required	(A) CAPITAL COST (inclusive of all taxes)	(B) AMC Cost for 2nd, 3rd, 4th & 5th year (Exclusive of Service Tax)	
			Software , Hardware.	Per Quarter	Total (for 16 Quarters)
	Correlation(DR)				
3	STORAGE (at DC)	N/A			
	STORAGE (at DR)	N/A			
4	Tape Library (at DC)	N/A			
	Tape Library (at DR)	N/A			
5	Database Activity Monitoring Tool (at DC)	Yes			
	Database Activity Monitoring Tool (at DR)	N/A			
6	Vulnerability Management Tool **(at DC only)**	N/A			
7	Standard Perforated Racks- (front & back) for entire solution at DC and DR	N/A		N/A	N/A
8	Accessories for entire solution (like L2 managed Switches, fiber cables, patch panels, patch cords, power strips etc.) for the racks	N/A			
9	OTHERS				

SL NO	Description	High Availability Required	(A) CAPITAL COST (inclusive of all taxes)	(B) AMC Cost for 2nd, 3rd, 4th & 5th year (Exclusive of Service Tax)	
			Software , Hardware.	Per Quarter	Total (for 16 Quarters)
TOTAL				X	
GRAND TOTAL (A+B)					

Indicative Price for scalability (will not be part of commercial)

1	Incremental cost for logger – for additional 2500 eps.	N/A	N/A		N/A		
2	Incremental cost for Correlation engine – for additional 2500 eps.	N/A	N/A		N/A		
3	Incremental cost for Storage – for additional 10 TB	N/A	N/A	N/A			

Note:

1. All the prices quoted above are inclusive of all taxes, etc.
2. The above price will remain valid for the terms of the contract.
3. Please provide price breakup of individual line items, if the line items comprises of various hardware/software/service components in above format.
4. Annual Maintenance charges for all the applicable line items have to be provided
5. The product costs mentioned in the price bid should include all the implementation related costs including but not limited to installation, integration, testing and operationalization of the item.
6. Annual Maintenance Charges (AMC) will include all costs but exclusive of service taxes such as AMC of hardware items, Annual recurring license fee, version upgrade, patch upgrade etc.
7. Complete project implementation methodology, deployment have to be provided. architecture, bill of material to be supplied for the above line items.
8. All prices are to be quoted by the Bidder.

9. All capacities defined in Bytes are native capacity unless specifically specified.
10. Bank reserves the right to negotiate on the indicative prices quoted by the successful bidder at the time of requirement for scaling up.
11. Self declaration stating that all the hardware items to be supplied, for the proposed solution as per RFP are not refurbished.

Note: Please Leave the space blank wherever the charges are not applicable.

Declaration by bidder: We, M/s _____, hereby confirm that all the items including Services as required for making system operational as per requirement of the Bank have been included in the commercial bid. Further, we understand that Bank reserve the right to use reverse auction method.

Prices of major components must be broken down.

Part B
Total Cost of Ownership Calculation format:

	Total cost
Fixed One time cost(Capital Cost)	
(a) Procurement & implementation	
Recurring/Incremental Cost(AMC Cost exclusive of Service Tax)	
2nd year	
3rd year	
4th year	
5th year	
(b) **Total Recurring Cost**	
Total Cost (a) +(b)	

Total Cost in **Part 'A'** and **Part B** should match.

Provide AMC/ License fee/ subscription fee/ Renewal fee details for each component of Hardware and Software and give year wise breakup during the -5- years time span.

Dated this ..... day of ..... 2012.....

.....
Signature
(In the Capacity of)

..... Duly authorised to sign bid for and on behalf of
(give below the Name & Address of Bidder with phone Numbers including local number and e mail address)

9.9. BILL OF MATERIAL

Please submit complete Bill of Material as per the following format for the materials to be supplied under this RFP preferably in Excel format including the proposed upgrade.

Sr. No.	Item Name	Make/ Model No.	Configuration/ Details/ Specifications	Brief Function of Item	Commercial Bid Line item (Leave blank if not applicable)	Qty	Page ref. no. of Brochure enclosed.	Remarks

Place:
Date: Seal and signature of the Bidder

9.10. Letter of authenticity

This has reference to "Implementation of a Comprehensive Log Management, Event Correlation and Database Activity Monitoring Solutions" being quoted to Indian Bank vide our quotation/order no. ----- Dated ----------.

We hereby undertake that all the components/parts/assembly/software used in the Entire solution and other supplies under the above, shall be original new components/parts/ assembly /software from respective OEMs of the products and that no refurbished/duplicate/ second hand components/parts/ assembly / software are being used or shall be used.

We also undertake that in respect of licensed operating system if asked by Indian Bank in the purchase order shall be supplied along with the authorised license certificate (eg. Product Keys on Certification of Authenticity in case of Microsoft Windows Operating System) and also that it shall be sourced from the authorised source (eg Authorised Microsoft Channel in case of Microsoft Operating System).

Should Indian Bank require, we shall produce certificate from our OEM supplier in support of above undertaking at the time of delivery/installation. It will be our responsibility to produce such letters from our OEM suppliers at the time of delivery or within a reasonable time.

In case of default and we are unable to comply with above at the time of delivery or during installation, for the supplies already billed, we agree to take back the supplies if already supplied and return the money if any paid to us by Indian Bank in this regard and our EMD/BG get forfeited.

We (system OEM Name/bidder) also take full responsibility of both Parts & Service SLA as per the content even if there is any defect by our Authorised Service Centre/Reseller etc.

Authorised Signatory

Name:

Designation

Place

Date

PS: (The above declaration has to be given by the company secretary duly Signed on the Letter Head of the company)

9.11. Format of NON DISCLOSURE AGREEMENT

THIS AGREEMENT made and entered into at ……..on this the…..day of……20.. between **INDIAN BANK**, a body corporate constituted under the Banking Companies (Acquisition & Transfer of Undertakings) Act 1970, having its Head Office at No.66, Rajaji Salai, Chennai, hereinafter called the "**BANK**" which term shall wherever the context so require includes its successors and assigns

AND

M/s. …….. Limited a company registered under the Companies Act having its registered office at…….. hereinafter called the " " which term shall wherever the context so require includes its successors and assigns, **WITNESSETH**:

WHEREAS

The Bank is interalia engaged in the business of banking and have been procuring computer systems and peripherals for its branches

M/s. ……..... Limited has been engaged in the business of ……
……
……. (indicate brief details of the company's business activities)

The parties intend to engage in discussions and negotiations concerning establishment of business relationship between themselves. In the course of discussions and negotiations, it is anticipated that the parties may disclose or deliver to the other certain or some of its trade secrets or confidential or proprietary information for the purpose of business relationship.

NOW THERFORE THIS AGREEMENT WITNESSETH and it is hereby agreed by and between the parties hereto as follows:

Confidential information-
Confidential information means all information disclosed/furnished by either party to another party in connection with the business transacted/ to be transacted between the parties. Confidential information shall include any copy, abstract, extract, sample, note or module thereof and electronic material or records.
Use of contract documents and information

M/s. ..... Limited shall not, without the Bank's prior written consent, disclose the Contract, or any provision thereof, or any specification, plan, drawing, pattern, sample or information furnished by or on behalf of the Bank in connection therewith, to any person other than a person employed by M/s..... Limited in the performance of the Contract. Disclosure to any such employed person shall be made in confidence and shall extend only as far as may be necessary for purposes of such performance.

M/s. ..... Limited shall not, without the Bank's prior written consent, make use of any document or information pertaining to this contract except for purposes of performing the Contract.

Receiving party may use the information solely for and in connection with the Purpose.

Use of Confidential Information-

Each party agrees not to use the other's confidential information for any purpose other than for the specific purpose. Any other use of such confidential information by any party shall be made only upon the prior written consent from the authorized representative of the other party or pursuant to subsequent agreement. between the Parties hereto.

The receiving party shall not commercially use or disclose for commercial purpose any confidential information or any materials derived therefrom, to any other person or entity other than persons in the direct employment of the Receiving Party who have a need to access to and knowledge of the confidential information solely for the purpose authorized above. The Receiving Party may disclose confidential information to consultants only if the consultant has executed non-disclosure agreement with the Receiving Party that contains terms and conditions that are no less restrictive than these and such consultant should also be liable to the original disclosing party for any unauthorized use or disclosure. The Receiving party shall take appropriate measures by instruction and written agreement prior to disclosure to such employees to assure against unauthorized use or disclosure. The Receiving Party agrees to notify the Disclosing Party immediately if it learns of any use or disclosure of the Disclosing party's confidential information in violation of the terms of this Agreement.

Neither party shall make news release, public announcements, give interviews, issue or publish advertisements or Agreement, the contents/provisions thereof, other information relating to this agreement, the purpose, the Confidential information or other matter of this agreement, without the prior written approval of the other party.

In case the Purchaser wishes not to renew the maintenance contract, after the term of this Agreement, the Purchaser has the right to maintain the System through its own employees. However, if the Purchaser wishes to appoint any entity other than the Supplier for providing the said maintenance services, the same can be done only after obtaining prior agreements from such entity with respect to protection of confidentiality and intellectual property rights of the Supplier. The entity shall provide such undertakings for protection of confidentiality and intellectual property rights as may be required by the Supplier by executing a form to be provided by the Supplier / Sub-Contractor. It is expressly understood that in such an event, the Purchaser undertakes at all times to protect the confidentiality and intellectual property rights of the Supplier and shall be responsible for all acts and deeds of the said entity.

3. Exemptions

The obligations imposed upon either party herein shall not apply to information, technical data or know-how whether or not designated as confidential, that:

- Is already known to the Receiving party at the time of the disclosure without an obligation of confidentiality
- Is or becomes publicly known through no unauthorized act of the Receiving party
- Is rightfully received from a third party without restriction and without breach of this agreement
- Is independently developed by the Receiving party without use of the other party's Confidential information and is so documented
- Is disclosed without similar restrictions to a third party by the Party owning the confidential information
- Is approved for release by written authorization of the disclosing party; or

- Is required to be disclosed pursuant to any applicable laws or regulations or any order of a court or a governmental body; provided, however that the Receiving party shall first have given notice to the Disclosing Party an made a reasonable effort to obtain a protective order requiring that the confidential information and / or documents so disclosed used only for the purposes for which the order was issued.

4. Term

This agreement shall be effective from the date of the execution of this agreement and shall continue till expiration or termination of this agreement due to cessation of the business relationship between the parties. Upon expiration or termination as contemplated herein the Receiving party shall immediately cease any or all disclosures or uses of confidential information and at the request of the disclosing party, the receiving party shall promptly return or destroy all written, graphic or other tangible forms of the confidential information and all copies, abstracts, extracts, samples, note or modules thereof.

The obligations of the receiving party respecting disclosure and confidentiality shall continue to be binding and applicable without limit until such information enters the public domain.

5. Title and Proprietary rights

Notwithstanding the disclosure of any confidential information by the disclosing party to the receiving party, the disclosing party shall retain title and all intellectual property and proprietary rights in the confidential information. No license under any trademark, patent or copyright or application for same which are or thereafter may be obtained by such party is either granted or implied by the conveying of confidential information.

6 .**Return of confidential information**

Upon written demand of the disclosing party, the receiving party shall (I) cease using the confidential information (ii) return the confidential information and all copies, abstracts, extracts, samples, note or modules thereof to the disclosing party within seven (7) days after
receipt of notice and (iii) upon request of the disclosing party, certify in writing that the receiving party has complied with the obligations set forth in this paragraph.

7. Remedies:-

The receiving party acknowledges that if the receiving party fails to comply with any of its obligations hereunder, the disclosing party may suffer immediate, irreparable harm for which monetary damages may not be adequate. The receiving party agrees that, in addition to all other remedies provided at law or in equity, the disclosing party shall be entitled to injunctive relief hereunder.

8. Entire agreement-

This agreement constitutes the entire agreement between the parties relating to the matter discussed herein and supersedes any and all prior oral discussion and/or written correspondence or agreements between the parties. This agreement may be amended or modified only with the mutual written consent of the parties. Neither this agreement nor any rights, benefits and obligations granted hereunder shall be assignable or otherwise transferable.

9. Severability

If any provision herein becomes invalid, illegal or unenforceable under any law, the validity, legality and enforceability of the remaining provisions and this agreement shall not be affected or impaired.

10. Dispute resolution mechanism:

In the event of any controversy or dispute regarding the interpretation of any part of this agreement or any matter connected with, arising out of, or incidental to the arrangement incorporated in this agreement, the matter shall be referred to arbitration and the award passed in such arbitration shall be binding on the parties. The arbitral proceeding shall be governed by the provisions of Arbitration and Reconciliation Act 1996 and the place of arbitration shall be Chennai.

11. Jurisdiction

The parties to this agreement shall submit to the jurisdiction of courts in Chennai.

12. Governing laws

The provisions of this agreement shall be governed by the laws of India.

In witness whereof, the parties hereto have set their hands through their authorised signatories

INDIAN BANK

M/s. …… Limited
(Vendor)

9.12. ESTIMATED EFFORT AND ELAPLSED TIME FOR THE PROJECT

Sl No	Activities	Elapsed Time	Effort in Man days	Number of team members who will be deployed	Remarks
1	Log Management And Event Correlation Solution Implementation				Please submit detailed implementation plan
2	Regular Management and Monitoring of proposed solutions to be deployed at DC & DR during business hours on working days	NA	NA		Please submit Manpower deployment plan as per your assessment
3	DAM Tool Implementation and regular monitoring				Please submit detailed implementation plan
4	Vulnerability Management tool implementation and monitoring				Please submit detailed implementation plan

Place:

Date: Seal and Signature of Bidder:

9.13. Documents to be submitted by the bidder

S.No.	Particulars of the Documents		
1.	Demand Draft payable at Chennai for Rs.10,000/- favouring "INDIAN BANK" towards Bid Document Price		
2.	Bid Security/Earnest Money Deposit in the form of Bank Guarantee for Rs. 10.00 lakhs (Rupees Ten lakhs only)		
3.	Copy of Valid Sales Tax/VAT Registration Certificate and Service Tax Registration Certificate		
4.	Copies of attested audited Balance Sheets for last 3 years, 2009-10, 2010-11, and 2011-12. (If audited BS for 2011-12 is not available, Audited BS of previous three years to be submitted)		
5.	Details of Projects executed		
6.	Letter of undertaking that the bidder is not in the blacklist of the Central/ any of the State Governments in India or any Financial Institution in India.		
7.	Soft copy of the documents		
8.	Complete solution document – should contain the following details		
	a	Architecture of the solution: This must contain details of implementation methodology of the project viz., Deployment of proposed Solutions with proposed time frame for each stage of the project along with details of manpower deployment.	
	b	Product details	
	c	Documentation of the products (software/firmware) to be deployed in the Solution along with Data Sheets, Details of Part Number and Fact Files pertaining to the appliances being quoted.	
	d	Details of OEM	
	e	Any other detail	
9	Bid form, Price schedules and Other Formats for submission		
	1	Technical Bid (should contain all the documents called for therein)	
	2	Manufacturer's Authorization form/Letter of Authorization/ letter of authority from the original equipment manufacturer. It should be on the letterhead of the manufacturer and should be signed by a person competent and having the power of attorney to bind the manufacturer	
	3	Bidder Profile	
	4	Clients' reference format	
	5	Bid Security Format	
	6	Contract Form	
	7	Performance Guarantee Form	
	8	Bill of Material	
	9	Letter of authenticity	
	10	Non Disclosure Agreement	
	11	Estimated effort and elapsed time for the project	

Note: This is only an indicative list and the bidder has to go through the entire RFP for complete set of documents to be submitted. Other documents as and when required during the technical evaluation should be submitted.