केनरा बैंक Canara Bank

REQUEST FOR PROPOSAL [RFP]

FOR

"SELECTION OF SECURITY SYSTEM INTEGRATOR TO SET UP INFORMATION SECURITY OPERATION CENTRE

IN

CANARA BANK"

Issued by: Canara Bank,
AP&M Group, 1st Floor,
DIT Wing, Naveen Complex,
14, MG Road, Bengaluru -560 001

केनरा बैंक Canara Bank

Bid Details in Brief

Sl. No.	Description	Details
1.	RFP No. and Date	RFP 05/2017-18 dated 26/05/2017
2.	Brief Description of the RFP	Selection of Security System Integrator to Setup Information Security Operation Centre in Canara Bank
3.	Bank's Address for Communication and Submission of Tender	Deputy General Manager Canara Bank, AP&M Group, 1st Floor, DIT Wing, Naveen Complex, 14 MG Road, Bengaluru -560 001 Tel - 080-25590070,25584873 Fax- 080-25596539 Email: hoditapm@canarabank.com Senior Manager, Asset Procurement & Management Group
4.	Date of Issue	26/05/2017, Friday
5.	Last Date of Submission of Queries for Pre Bid Meeting	05/06/2017, Monday, 3.00 PM
6.	Date of Pre Bid Meeting	07/06/2017, Wednesday, 3.00 PM
7.	Last Date of Submission of Bids	26/06/2017, Monday upto3.00 PM
8.	Date and time of Opening of Part A- Conformity to Eligibility Criteria.	26/06/2017, Monday, 3.30 PM
9.	Date and time opening of Technical Bid Part-B/Commercial Bid	Will be intimated at a later date.
10.	Application Fees (Not Refundable)	Rs.25,000/-
11.	Earnest Money Deposit(Refundable)	Rs.75,00,000/-

This document can be downloaded from Bank's website http://canarabank.com/english/announcements/tenders. In that event, the bidders should pay the Application Fee for tender document by means of DD drawn on any scheduled Commercial Bank for the above amount in favor of Canara Bank, payable at Bengaluru and submit the same along with the Bid document.

DISCLAIMER

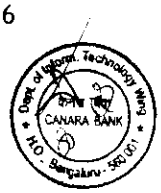
The information contained in this Request for Proposal ("RFP") document or information provided subsequently to bidders or applicants whether verbally or in documentary form by or on behalf of Canara Bank (or Bank), is provided to the bidder(s) on the terms and conditions set out in this RFP document and all other terms and conditions subject to which such information is provided. This RFP document is not an agreement and is not an offer or invitation by Canara Bank to any parties other than the applicants who are qualified to submit the bids (hereinafter individually and collectively referred to as "Bidder" or "Bidders" respectively). The purpose of this RFP is to provide the Bidders with information to assist the formulation of their proposals. This RFP does not claim to contain all the information each Bidder requires. Each Bidder may conduct its own independent investigations and analysis and is free to check the accuracy, reliability and completeness of the information in this RFP. Canara Bank makes no representation or warranty and shall incur no liability under any law, statute, rules or regulations as to the accuracy, reliability or completeness of this RFP. The information contained in the RFP document is selective and is subject to updating, expansion, revision and amendment. It does not purport to contain all the information that a Bidder requires. Canara Bank does not undertake to provide any Bidder with access to any additional information or to update the information in the RFP document or to correct any inaccuracies therein, which may become apparent.

Canara Bank reserves the right of discretion to change, modify, add to or alter any or all of the provisions of this RFP and/or the bidding process, without assigning any reasons whatsoever. Such change will be published on the Bank's Website (**http://canarabank.com/english/announcements/tenders**) and it will become part and parcel of RFP.

Canara Bank in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP. Canara Bank reserves the right to reject any or all the Request for Proposals received in response to this RFP document at any stage without assigning any reason whatsoever. The decision of Canara Bank shall be final, conclusive and binding on all the parties.

Abbreviations used in this Document:

1.	AMC	Annual Maintenance Contract
2.	ATS	Annual Technical Support
3.	BG	Bank Guarantee
4.	BOM	Bill of Material
5.	CST	Central Sales Tax
6.	DD	Demand Draft
7.	DIT	Department of Information Technology
8.	EMD	Earnest Money Deposit
9.	HO	Head Office
10.	HTTP	Hyper Text Transfer Protocol
11.	HTTPS	Hyper Text Transfer Protocol Secure
12.	ISDN	Integrated Services Digital Network
13.	ITU	International Telecommunication Union
14.	LAN	Local Area Network
15.	LD	Liquidated Damage
16.	LST	Local Service Tax
17.	MAF	Manufacturer Authorisation Form
18.	MSME	Micro Small & Medium Enterprises
19.	MTBF	Mean Time Between Failure
20.	MTTR	Mean Time To Restore
21.	NEFT	National Electronic Funds Transfer
22.	NI Act	Negotiable Instruments Act
23.	OEM	Original Equipment Manufacturer
24.	OS	Operating System
25.	PDI	Pre Delivery Inspection
26.	PERT	Project Execution and Review Technique
27.	RFP	Request For Proposal [Interalia the term 'Tender' is also used]
28.	RTGS	Real Time Gross Settlement
29.	DAM	Database Activity Monitoring
30.	DLP	Data Leakage Prevention
31.	VM	Vulnerability Management solution
32.	PIM	Privileged Identity Management
33.	NBA	Network Behavior Analysis



LIST OF CONTENTS

17.	Annexure-4 Technical Bill of Material
18.	Annexure-5 Masked Commercial Bill of Material (By masking the Price)
19.	Annexure-6 Resource Plan Matrix for SOC operations
ANNEXURES(To be submitted with Part-C -Commercial Bid)	
20.	Format-14 Covering letter format for Commercial Bid
21.	Annexure-5 Commercial Bill of Material

APPENDICES	
A.	Instructions to be noted while preparing/submitting Part A- Conformity to Eligibility Criteria
B.	Instructions to be noted while preparing/submitting Part B- Technical Proposal
C.	Instruction to be noted while preparing/submitting Part C-Commercial Bid
D.	Bank Guarantee Format for Earnest Money Deposit
E.	Proforma of Bank Guarantee for Contract Performance
F.	Format for Sending Pre-Bid Queries
G.	Pre Contract Integrity Pact

A. INTRODUCTION

1. About Canara Bank

CANARA BANK, a body Corporate and a premier Public Sector Bank established in the Year 1906 and nationalized under the Banking Companies (Acquisition and Transfer of Undertakings) Act, 1970, having its Head office at 112, J C Road Bengaluru-560002 and among others, having DIT Office at Naveen Complex, No.14, M G Road, Bengaluru-560001. The Bank is having pan India presence of more than 5900 branches,21 Circle offices and 118 Regional Offices situated across the States. The Bank is working on Core Banking System using Flex cube solutions. The Bank is a forerunner in implementation of IT related products and services and continuously making efforts to provide the state of art technological products to its customers.

2. Definitions

2.1. 'Bank' means unless excluded by and repugnant context or the meaning thereof, shall mean 'Canara Bank', described in more detail in paragraph 1 above and which has invited bids under this Request for Proposal and shall be deemed to include its successor and permitted assigns.

2.2. 'RFP' means Request for Proposal for Supply, Installation, Implementation, Commissioning and Maintenance of Security Operations Centre Solution in Canara Bank.

2.3. 'Bidder' means a vendor submitting the proposal in response to RFP.

2.4. 'Solution' means setting up of information Security Operation Centre Solution in Canara Bank.

2.5. 'Contract' means the agreement signed by successful bidder and the Bank at the conclusion of bidding process, wherever required.

2.6. 'Successful Bidder'/ 'H1 bidder' means the Bidder who is found to be the highest scored bidder after conclusion of the bidding process, subject to compliance to all the Terms and Conditions of the RFP, etc.

3. About RFP

3.1. Considering the fast paced threats in the IT environment, Canara Bank has decided to strengthen its Information Security set up as per the guidelines in the Gopalakrishnan Committee report on IT Security (Circular DBS.CO.ITC.BC.No.6/31.02.008/2010-11), released on 29th April, 2011 and RBI circular DBS.CO/CSITE/BC.11/33.01.001/2015-16 dated 2nd June, 2016. The objective of this RFP is to find a suitable system integrator who has worked previously in delivering similar projects in the banking or related industry verticals. Canara Bank, hereafter called as "Bank", expects all bidders, having proven experience in the area of IT security/SOC implementation, as system integrator of in- scope solutions, to respond to this RFP.

3.2. Note: This RFP should not be considered as a statement of intent for procurement, unless a purchase order or notification of award is published by Canara Bank if any, as an end result of this RFP process.

3.3. This RFP document is meant for the exclusive purpose of "Setting up of Information Security Operation Center" at Canara bank as per the terms, conditions and specifications indicated and shall not be transferred, reproduced or otherwise used for purposes other than for which it is specifically issued.

4. Objective

4.1. Intended Architectural principles of the SOC:

The Architectural principles that form the underlying platform for the SOC implementation at Canara bank is as mentioned below. The solutions and their deployment architecture follow from these principles. The "bidder" herein after called as "System Integrator" or "vendor "or "SI", is expected to adhere to these principles while submitting their response;

4.2. Functional Principles:

The intent for implementing a SOC at Canara Bank is covered in the below functional principles:

a. Identification & Prevention of Information Security Vulnerabilities: The SOC should be able to identify information security vulnerabilities in Canara Bank environment and prevent these vulnerabilities through implementation of adequate security solutions or controls.

b. Incident Management: Reporting and logging of information security incidents, track and monitor the closure of these information security incidents and escalation of these incidents to appropriate teams/ individuals in the bank if required. Documentation of Incidents along with their root cause to build a known database of incidents to refer in future.

c. Continuous Improvement: Continuously improve SOC operations.

4.3. Scalability Principles:

The solutions deployed should be modular, scalable and should be able to address Canara Bank requirements for the next five years, with the deployed hardware.

4.4. Availability Principles:

The solutions and services in scope should be designed with adequate redundancy and fault tolerance to ensure compliance with SLAs for uptime, as outlined in this RFP.

4.5. Performance Principles:

The solutions should not have a significant impact on the existing infrastructure of Canara Bank either during installation or during operation of SOC.

4.6. Forensics and Deep Packet Analysis:

Dynamic Behavior Analysis - Preliminary static and dynamic analysis and collecting Indicators of Compromise (IOC).

4.7. Based on the architectural principles, The Bank proposes to procure the following solutions to enhance the security posture of Canara Bank to enable Security Operations Monitoring as per the Terms & Conditions, Technical Specifications and Scope of Work described elsewhere in this document.

a. Security Operations Centre (SOC) with Security Information and Event Management Solution (SIEM)
b. Data Leakage Prevention (DLP)
c. Database Activity Monitoring (DAM)
d. Privilege Identity Management solution (PIM)
e. Anti-Advance Persistent Threat (Anti-APT)
f. Vulnerability Management and Scanner

g. Network Behavior Analysis (NBA)
h. Anti-DDoS

4.8. The Bidders who wish to take up the project shall be responsible for the following:

a. Procurement of the necessary solutions and the corresponding hardware, software, database etc. required for implementing these solutions at Canara bank.
b. Implementation of the respective solutions at Canara bank including configuration, customization of the products as per the Bank's requirement.
c. Integration of the solutions to provide a comprehensive single dashboard view of the security risks/ incidents for Canara bank.
d. The bidders must ensure that solution procured, their configuration and operations should comply with the current statutory/regulatory requirements and also those during the contract period.
e. Work with the existing System Integrator(s) of Canara Bank to integrate the SOC solutions with existing application platforms, server and storage environment, enterprise network, EMS/ NMS solutions, security solutions, ticketing tools etc.
f. Providing adequate resources for on-going operations of the Security Operations Center (SOC).
g. Development of operating procedures in adherence with Canara bank's policies.
h. Adherence to agreed Service Level Agreements (SLA) and periodic monitoring and reporting of the same to Canara bank.
i. Continual improvement of the Security Operations as defined in the SLA.

5. Eligibility Criteria:

5.1. A vendor submitting the proposal in response to this RFP shall hereinafter be referred to as 'Bidder' and setting up of Security Operation Centre in Canara Bank in the Bank shall hereinafter be referred as "Solution".

5.2. Only those bidders who fulfill the pre-qualification criteria for bidder and OEMs as mentioned in **Annexure-1** are eligible to submit response to this RFP.

5.3. The bidder is required to provide factually correct responses to the RFP. Adequate justification for the response (including the technical and other requirements) should be provided as part of the response. In case the bank finds any response to be inadequate, the bank has the right to ask for additional explanation/justification. In the event of any discrepancy in the response submitted by the bidder, the bank reserves the right to disqualify/blacklist the bidder and the OEM.

5.4. Canara bank, reserves the right to change or relax the eligibility criteria to ensure inclusivity.

5.5. Canara Bank, reserves the right to verify/evaluate the claims made by the bidder independently. Any deliberate misrepresentation will entail rejection of the offer.

5.6. The bidder can be part of only one bid.

5.7. In case an OEM submits a bid as a bidder, then the OEM cannot participate through other system Integrator bids.

5.8. System integrator of CBS in Canara Bank is not eligible to apply

Note: The bidder can propose products from different OEMs for the other solutions in scope (Example: Bidder "A" can propose products from OEMs "B", "C" etc. for DAM, WAF etc.)

D.I.T. Wing, A P & M Group CANARA BANK H.O. Bengaluru - 560001

6. Participation Methodology:

6.1. In a tender either the partner/distributor/System Integrator on behalf of the OEM or OEM itself can bid but both cannot bid simultaneously for the same item/product in the same tender.

6.2. If a partner/distributor/System Integrator bids on behalf of the OEM, the same partner/distributor/System Integrator shall not submit a bid on behalf of another OEM in the same tender for the same item/product.

6.3. System integrator of CBS in Canara Bank is not eligible to apply.

6.4. In the event partner/distributor/System Integrator fails in their obligations to provide the product updates (including management software updates and new product feature releases) within 30 days of release/announcement, the OEM should assume complete responsibility on behalf of the partner/distributor/System Integrator to provide the same to the bank at no additional cost to the bank and will directly install the updates, upgrades and any new product releases at the Bank's premises. To this effect Bidder should provide a dealer/distributor certificate as per **Format-13**.

7. Existing Infrastructure:

7.1. Canara Bank Department of Information Technology wing is presently using manual methods for the management of the end points like servers etc. Detailed information about the Bank's existing infrastructure is mentioned in the **Annexure-7**.

8. General Scope of Work for each solution:

8.1. Bank invite sealed offers ('Conformity to Eligibility Criteria', 'Technical Proposal' and 'Commercial Bid') for Supply, Installation, Implementation, Commissioning and Maintenance of Security Operations Centre Solution for Department of Information Technology Wing of the Bank for its DC & DRC setup located at Bengaluru and Mumbai respectively as per the Terms & Conditions, Technical Specifications and Scope of Work described elsewhere in this document.

8.2. Detailed technical specification for each of in-scope Solution is furnished in **Annexure-2**. All the Hardware/Software ordered for Supply, Installation and Maintenance of Security Operations Centre Solution and other Items should have comprehensive onsite warranty of 3 years and AMC/ATS Period of 3 Years (if Contracted).

8.3. Bank reserves the right to increase or decrease the quantum of purchase by 25% in respect to the quantity specified in this tender at the same rate arrived at on the Terms and Conditions of this Tender.

8.4. This section refers to the broad set of requirements for all solutions to be deployed at Canara bank. Detailed scope of work for each solution is mentioned separately in **Annexure-7**: Scope of Work. For the solutions in scope, the bidder may propose any appliance or software or appliance plus lightweight agent based (as applicable) solution along with necessary hardware.

8.5. In case of software based solution, the bidder needs to propose at a minimum the below hardware:

8.5.1. For SIEM:

a. Minimum of 16 cores (Intel Xeon E5 based chip) and 32 GB of RAM and should be expandable to minimum 32 cores and 128 GB of RAM.

DIT Wing A P & M Group CANARA BANK H.O. Bengaluru - 560 001

b. All servers should at a minimum have 600 GB redundant Hard-disk @ 10000 RPM or latest version of RPM.

8.5.2. For other solutions (software based), the minimum server sizing expected is:

a. Intel Xeon quad core processor 2.4 GHz with 16GB Ram (Rack mountable).
b. All servers should at a minimum have 600 GB redundant Hard-disk @ 10000 RPM or the latest version of RPM.

8.5.3. For any management servers the deployment requirement is for DC in HA and standalone in DR. These should be in 1U size and should have the following configuration:

a. Intel Xeon quad core processor 2.4 GHz,8GB expandable to minimum 16 GB RAM.

8.5.4. The bidders are free to quote blade servers to meet the requirements of this RFP; however the OEMs for these servers must be in the leader's quadrant for this year's or previous years (2017 or 2016 or 2015 whichever is latest) Gartner Magic Quadrant for Blade servers.

8.5.5. The Server make proposed should be from reputed manufacturers (data center class) and should have been deployed by the bidder in other organizations. All servers should meet the below mentioned criteria:

a. Server family should have published benchmark SPECint rate and SPECfb rate benchmark.
b. Server family should have published benchmark TPC benchmark.
c. Server should have 4*1G integrated on-board ports and should support two embedded 10 Gb Ethernet ports (10GBASE-T RJ-45 or 10GBASE-SR SFP+ based) without consuming PCIe slots.
d. Should be in the top 5 of IDC's latest worldwide server market review report.

8.5.6. The above is only the minimum requirement and the actual sizing of the servers should be based on the scope of the bank and SLAs as defined in this RFP. Bidder is responsible for sizing the infrastructure required for the in-scope activities under this RFP.

a. The bidder shall ensure that the hardware proposed does not reach end of life during the contract period.
b. The bidder shall ensure that any additional hardware/software/network equipment required to operationalize the respective solutions/devices must be detailed in the technical and commercial bill of material. If the same is not ensured, the bidder shall be responsible to provide such hardware/software/networking equipment free of cost to the bank at the time of implementation. The above details should be treated as a baseline and the bidder is required to size the hardware as per the 'Scope of Work' annexure-7 as per this RFP. The bidder is expected to provide calculations/ logic arrived at the sizing for all appliances/ hardware as part of the response.

8.6. Security Information & Event Management (SIEM)

The SIEM solution is expected to collect logs from security and network devices, servers and application security logs. In addition, the logs being generated by the solutions deployed as part of the SOC implementation need to be collected by the SIEM. The bidder is expected to perform the following as part of the SIEM:

8.6.1. Solution Implementation:

a. Implement the SIEM tool to collect logs from the identified devices/applications/databases etc.
b. Develop parsing rules for non-standard logs.
c. Implement correlation rules based on out-of-box functionality of the SIEM solution and also based on the use-cases defined in the RFP.

8.6.2. Training:

a. Provide training to the identified bank personnel/ SOC team on the product architecture, functionality and the solution design - to be provided before the implementation of solution.
b. Provide hands-on training to the bank personnel/ SOC team on SIEM policy configuration, alert monitoring, and etc. post implementation.

8.6.3. Ongoing Operations:

a. Monitor the SIEM alerts and suggest/ take appropriate action as per the SLA defined in the RFP.
b. Perform on-going optimization, performance tuning, maintenance, configure additional use- cases, suggest improvements as a continuous improvement process.
c. Perform log backup and archival as per Canara bank's policy requirements, and applicable legal/ statutory requirements.
d. Ensure that SLA's are maintained as defined in the RFP.

8.6.4. SOC Monitoring:

8.6.4.1. The SIEM should be able to collate logs from the devices/applications/databases etc. mentioned in the scope as per the Annexure7, including the solutions deployed as part of this RFP at Canara Bank. The configured correlation alerts should be displayed on LED display maintained at the SOC.

8.6.4.2. The bidder should also quote for minimum 60" LED display screens at the SOC. In addition, the bidder should quote for desktops with dual VGA cards/ dual monitors and a minimum of 8 GB RAM for the SOC monitoring team.

8.6.4.3. The bidder must also provide for all cabling including fiber cabling to connect the SOC to the DC/DR/ connecting office.

8.6.4.4. The Bidder shall provide estimates of the power, cooling, space, seating/furniture requirements, for Canara bank. Canara bank shall be responsible for providing these.

8.6.4.5. The bidder shall provide Video Matrix Switch which routes video from computers (Dual Monitors) in SOC room to multiple displays (projectors, monitors, etc.). All necessary configuration/implementation of this network is also Bidders Responsibility. The same needs to be covered under the ICB / Bill of materials in Technical bid with Models and specifications.

8.6.5. Integration:

The SIEM tool should be integrated with incident management/ ticketing tool to generate automated tickets along with criticality levels for the alert events generated by the SIEM tool. All the security devices/solutions being proposed as part of the current RFP/existing security devices and solutions identified by the bank need to be included for monitoring by SIEM solution.

8.6.6. Replication:

The logs collected by the SIEM log collector should be replicated across primary Data Canter, Disaster Recovery and Near DR location. The bidder needs to provide an estimate of the bandwidth required for the replication process after due analysis of the existing setup of Canara bank. Canara bank shall procure additional bandwidth if required. The bidder should ensure that there should be no data loss across DC and DR. The logs should be in sync across DC and DR.

8.6.7. Storage:

8.6.7.1. The SIEM should be able to maintain 3 months of logs on-box. In addition, the bidder should provide near line storage i.e. secondary storage for archiving logs for up to 12 months and offline storage for storage of logs for up to 4 years. Total 5 years logs must be available excluding the 3 months logs on-box. The bidder is responsible for sizing the storage adequately based on the EPS estimate given in the detailed scope of work.

8.6.7.2. The bidder should provide the storage for initial two years during the deployment and the storage for the rest of the three years should be delivered three months before the completion of second year.

8.6.7.3. The bidder is free to quote either of SAS/SSD for tier 1 storage and SATA/SAS/SSD for tier 2 which meet the requirements.

8.6.7.4. The bidders should provide details of the calculations used to arrive at the sizing as part of the response. The bidder is responsible for automated online replication of logs (online/ archival) from DC to DR for redundancy.

8.6.7.5. The solution should be capable of automatically moving the logs from online to archival storage based on the ageing of the logs. The solution should support object storage to provide protection from attacks such as Ransomware.

8.6.7.6. The logs should be stored in tamper proof mechanism for online and archival storage. The archival storage should have "Write Once Read Many (WORM)", Encryption (or) Hashing, Index and Search, Retention and Disposal functionality-Compression. The solution should have the option to support backup on tape library.

8.6.7.7. The expected storage requirements at a minimum are mentioned below. However, the bidder is expected to size the storage as per the requirements mentioned in the 'Scope of Work' Annexure 7 in this RFP. The bidder's response should include the calculations/ logic used to arrive at the sizing.

Table 1: Minimum Storage Requirements

Tier	Type	Disk RPM	RAID
Tier-I	SAN(SAS/SSD)	15000 (or the latest version available)	5
Tier-II	Archival (4years), SAN Based with deduplication/ compression capability(SATA/ SAS/SSD)	7200 (or the latest version available)	5

8.6.7.8. The bidder is free to quote the maximum storage to meet the Bank's requirement. In case additional storage is required then the bidder is liable to procure the additional storage at no additional cost to the Bank.

8.6.7.9. All storage devices should include at a minimum a dual controller and should be of the following specifications with respect to host connectivity:

Table 2: Minimum Host Connectivity Requirements

Host Connectivity	1GBE iSCSI	2 Ports/Controller
	10GB iSCSI	2 Ports/Controller
	8GB FC	4 Ports/Controller
Archival storage Connectivity	Protocols to be supported: CIFS,NFS &HTTP.	

8.6.7.10. The solution should also be scalable to expand storage based on the peak EPS requirement of Canara bank. The bidder is expected to provide all supporting infrastructure for management of the storage devices such as switches (NAS/SAN), controllers etc. and these are to be provided at the time of implementation supporting the maximum scalability as defined above.

8.6.7.11. It is the responsibility of the SI to quote for adequate storage depending on the Bank's storage requirement for the logs. In the event it is found that the storage quoted by the SI is not sufficient, the SI will have to procure additional storage to meet the Bank's requirement at no additional cost to the Bank.

8.6.8. Packet Capture:

8.6.8.1. The Solution must be capable of full packet capture and securely store these packets for a minimum of 30 days.

8.6.8.2. Raw packets are to be stored for a period of 15 days and meta-data to be stored for a period of 30 days.

8.6.8.3. The solution should not have any restriction on the maximum packet size that can be captured.

8.6.8.4. The solution should have the ability to selectively store packets captured in an external storage provided by the Bank.

8.6.9. Incident Management Tool:

8.6.9.1. The solution should be able to register any security event and generate trouble ticket.

8.6.9.2. The solution should provide complete life cycle management (work flow) of trouble tickets from incident generation till closure of the incident.

8.6.9.3. The solution should provide the logging facility to different levels of users to monitor and manage the incidents generated for closure of the same as per the defined workflow.

8.6.9.4. The proposed solution should be able to integrate all the security devices/solutions being proposed as a part of the current RFP/existing security devices and solutions identified by the bank.

8.6.9.5. The Incident management should include escalation as per the escalation matrix.

8.6.9.6. The solution should be able to send the incident report in various forms like e-mail, SMS etc.

8.7. Data Loss Prevention (DLP)

DLP too should be able to detect potential data breaches/data ex-filtration transmissions and prevent them by monitoring, detecting and blocking sensitive data while in-use, in-motion and at-rest.

The bidder is required to perform the following activities for implementing the DLP in the bank:

8.7.1. Solution Implementation:

8.7.1.1. Deploy the network DLP in a listening mode/ inline mode (as per Canara bank's requirement) to identify the traffic movement.
8.7.1.2. Analyze the traffic movement and suggest policies / procedures to control data leakage.
8.7.1.3. Identify the location of sensitive information using the Discovery module.
8.7.1.4. Suggest policies for DLP implementation at end point level.
8.7.1.5. Implement the End point DLP solution based on the agreed policy.

8.7.2. Training:

8.7.2.1. Provide training to the identified bank personnel/ SOC team on the product architecture, functionality and the solution design - to be provided before the implementation of solution.
8.7.2.2. Provide hands-on training to the bank personnel/ SOC team on DLP policy configuration, alert monitoring, and etc. post implementation.

8.7.3. Solution Integration:

8.7.3.1. Integrate DLP with SIEM solution to provide a single view of events generated.
8.7.3.2. The primary responsibility of integration of solution with SIEM lies with the SI selected through this RFP. Adequate support shall be provided by the existing system integrator for the purpose of integration.

8.7.4. Monitoring:

8.7.4.1. Monitor events from DLP and suggest/ take appropriate action to the bank on an on-going basis.
8.7.4.2. Improve the policies configured on an on-going basis to reduce the occurrence of false positives.

8.8. Database Activity Monitoring (DAM)

DAM is required for monitoring and analyzing database activity that operates independently of the DBMS. DAM should perform continuously and in real-time. DAM tools should use several data collection mechanisms (such as server-based agent software and in-line or out-of-band network collectors), aggregate the data in a central location for analysis, and report based on behaviors that violate the security policies and/or signatures or indicate behavioral anomalies. DAM tool should support for privileged user monitoring to address compliance-related audit findings, and by threat-management requirements to monitor database access.

The bidder is expected to perform the following activities:

8.8.1. Solution Implementation:

8.8.1.1. Deploy the DAM for DC and DR locations for the in-scope databases.
8.8.1.2. Configure the DAM rules and policies.

8.8.2. Training:

8.8.2.1. Provide training to the identified bank personnel/ SOC team on the product architecture, functionality and the solution design - to be provided before the implementation of solution.

8.8.2.2. Provide hands-on training to the bank personnel/ SOC team on DAM policy configuration, alert monitoring, and etc. post implementation.

8.8.3. Solution Integration:

8.8.3.1. Integrate DAM with SIEM solution to provide a single view of events generated.

8.8.3.2. The primary responsibility of integration of solution with SIEM lies with the SI selected through this RFP. Adequate support shall be provided by the existing system integrator for the purpose of integration.

8.8.4. Monitoring:

8.8.4.1. Monitor events from DAM and suggest/ take appropriate action to the bank on an on-going basis.

8.8.4.2. Improve the policies configured on an on-going basis to reduce the occurrence of false positives.

8.9. Privileged Identity Management (PIM)

A privileged Identity Management technology needs to accommodate for the special needs of privileged accounts, including their provisioning and life cycle management, authentication, authorization, password management, auditing, and access controls. Tool should protect, automate and audit the use of privileged identities to help thwart insider threats and improve security across the extended enterprise.

The bidder is expected to perform the following activities:

8.9.1. Solution Implementation:

8.9.1.1. Implement the solution for the identified devices.

8.9.2. Training:

8.9.2.1. Provide training to the identified bank personnel/ SOC team on the product architecture, functionality and the solution design - to be provided before the implementation of solution.

8.9.2.2. Provide hands-on training to the bank personnel/ SOC team on PIM operations - post implementation.

8.9.3. Solution Integration:

8.9.3.1. Integrate PIM with SIEM to generate alerts for any PIM violations.

8.9.3.2. The primary responsibility of integration of solution with SIEM lies with the SI selected through this RFP.

8.9.4. Monitoring:

8.9.4.1. Monitor events from PIM and suggest/ take appropriate action to the bank on an on-going basis.

8.9.4.2. Improve the policies configured on an on-going basis to reduce the occurrence of false positives.

8.10. Anti-Advanced Persistent Threat System (Anti-APT)

The bidder is expected to perform the following activities:

8.10.1. Solution Implementation:

8.10.1.1. Implement the solution for the identified devices

8.10.2. Training:

8.10.2.1. Provide training to the identified bank personnel/ SOC team on the product architecture, functionality and the solution design - to be provided before the implementation of solution.

8.10.2.2. Provide hands-on training to the bank personnel/ SOC team on Anti-APT operations post implementation.

8.10.3. Solution Integration:

8.10.3.1. Integrate anti-APT with SIEM solution for any Anti-APT violations.

8.10.3.2. The primary responsibility of integration of solution with SIEM lies with the SI selected through this RFP.

8.10.4. Monitoring:

8.10.4.1. Monitor events from Anti-APT and suggest/ take appropriate action to the bank on an on-going basis.

8.10.4.2. Improve the policies configured on an on-going basis to reduce the occurrence of false positives.

8.11. Vulnerability Management and Scanner

The bidder is expected to perform the following activities:

8.11.1. Solution Implementation:

8.11.1.1. Deploy the Vulnerability Management and assessment Scanner to monitor the critical devices.

8.11.1.2. Configure the VM policies.

8.11.2. Training:

8.11.2.1. Provide training to the identified bank personnel/ SOC team on the product architecture, functionality and the solution design - to be provided before the implementation of solution.

8.11.2.2. Provide hands-on training to the bank personnel/ SOC team on VMpolicy configuration, alert monitoring, and etc. post implementation.

8.11.3. Solution Integration:

8.11.3.1. Integrate VMwith SIEM solution to provide a correlated view of threats and vulnerabilities associated with them along with remediation mechanism.

8.11.3.2. The primary responsibility of integration of solution with SIEM lies with the SI selected through this RFP.

8.12. Network Behavior Analysis (NBA)

The network behavior analysis module is required to identify the abnormalities in the bank's network behavior. The bidder is expected to perform the following activities:

8.12.1. Solution Implementation:

8.12.1.1. Deploy the NBA for DC and DR locations.

8.12.1.2. Identify network baseline and configure the NBA policies

8.12.2. Training:

8.12.2.1. Provide training to the identified bank personnel/ SOC team on the product architecture, functionality and the solution design - to be provided before the implementation of solution.

8.12.2.2. Provide hands-on training to the bank personnel/ SOC team on NBA policy configuration, alert monitoring, and etc. post implementation.

8.12.3. Solution Integration:

8.12.3.1. Integrate NBA with SIEM solution to provide a correlated view of events generated.

8.12.3.2. The primary responsibility of integration of solution with SIEM lies with the SI selected through this RFP.

8.12.4. Monitoring:

8.12.4.1. Monitor events from NBA and suggest/ take appropriate action to the bank on an on-going basis.

8.12.4.2. Improve the policies configured on an on-going basis to reduce the occurrence of false positives.

8.13. Anti-DDoS

The Anti-App DDoS module is expected to constantly monitor the behavior of the application visitors and prevent common application layer attacks such as HTTP floods, Slowloris, Apache Killer etc. The bidder is expected to perform the following activities:

8.13.1. Solution Implementation:

8.13.1.1. Deploy the Anti-DDoS solution for DC and DR locations.

8.13.2. Training:

8.13.2.1. Provide training to the identified bank personnel/ SOC team on the product architecture, functionality and the solution design - to be provided before the implementation of solution.

8.13.2.2. Provide hands-on training to the bank personnel/ SOC team on Anti-DDoS operations - post implementation.

8.13.3. Solution Integration:

8.13.3.1. Integrate Anti-DDoS with SIEM to generate alerts for any Anti-DDoS violations.

8.13.3.2. The primary responsibility of integration of solution with SIEM lies with the SI selected through this RFP.

8.13.4. Monitoring:

8.13.4.1. Monitor events from Anti-DDoS and suggest/ take appropriate action to the bank on an on-going basis.

8.13.4.2. Improve the policies configured on an on-going basis to reduce the occurrence of false positives.

9. General Responsibilities of the SI

9.1. Training

9.1.1. Pre-Implementation: Provide training to the identified bank personnel/ SOC team on the product architecture, functionality and the design for each solution under the scope of this RFP.

9.1.2. Post Implementation: Provide hands-on training to the bank personnel/ SOC team on SIEM operations, alert monitoring, policy configuration for all solutions etc.

9.1.3. The bidder is also responsible for conducting annual training to the identified persons in the Bank.

9.1.4. The bidder and OEM are required to provide training jointly as per the below table for 20 people nominated by the bank for each solution specified in the scope of work irrespective of the location of the people. Further, the bank may choose to carry out training for different solutions at different locations.

9.1.5. The bidder is required to provide all trainees with detailed training material and 3 additional copies to Canara Bank for each solution as per the scope of work. This training material should cover installation, operation, integration, maintenance, troubleshooting and other necessary areas for each solution.

9.1.6. The bidder may utilize the OEM resources in case the bidder does not have adequately experienced resources for providing training.

Table 3: Training Requirements

Solution	Training Type		Days
	Pre- Implementation	Post- Implementation	
SIEM	Yes		2
		Yes	5
DLP	Yes		1
		Yes	3
DAM	Yes		1
		Yes	2
PIM	Yes		1
		Yes	2
Anti-APT	Yes		1
		Yes	1
VM	Yes		1
		Yes	1
NBA	Yes		1
		Yes	2
Anti-DDoS	Yes		1
		Yes	1

9.2. Implementation & Integration

9.2.1. Implementation of the specified solutions and necessary hardware requested by Bank and as per the technical requirement of the solutions which are detailed in Annexure -2. Selected bidder to ensure that the proposed solution complies with all the technical requirements (Annexure 2) post implementation of each solution to which the bidder responds as "Yes" in Annexure 2.

9.2.2. 10 days before delivery of the solutions, the bidder is required to review the bank environment and specify any additional requirements that the bank may need to provide for the implementation of the solution.

9.2.3. The bidder is responsible to ensure that the SOC solutions and operations comply with Canara bank's information security policies and industry leading standards (such as ISO 27001 etc.) and any applicable laws and regulations.

9.2.4. In addition, the bidder is responsible for impact assessment and modification of SOC operations at no extra cost, on account of any changes to applicable information security policies/ procedures / standards/ regulations.

9.2.5. The support for all the solutions proposed should be provided for minimum 5 years. Whereas free upgrade should be provided for all solutions if the end of life occurs within the period of contract with Canara bank. The Updates/ Upgrades should be implemented within 3 months of release of the same.

9.2.6. Integrate each solution with SIEM solution to provide a single view of events generated.

9.2.7. Any interfaces required with existing applications/ infrastructure within the bank should be developed by the bidder for successful implementation of the SOC as per the defined scope of work.

9.2.8. The Bidder should ensure that any changes made to any of the proposed solutions in DC are reflected in DR in near real-time.

9.2.9. Bidder shall be responsible for timely compliance of all Device level audit (DLA) and Vulnerability Assessment (VA) audit observations as and when shared by the bank.

9.2.10. Post initial implementation, the bidder is responsible for integrating any additional logs that the bank may wish to monitor with the SIEM solution at no additional cost to the bank.

9.2.11. The primary responsibility of integration of solution with SIEM lies with the SI selected through this RFP. The SI is responsible to co-ordinate with the existing System Integrator for the successful integration and implementation. Adequate support shall be provided by the existing system integrator for the purpose of integration.

9.2.12. Development and implementation of processes for management and operation of the SOC including (but not limited to) the following processes:

- **9.2.12.1.** Configuration and Change Management.
- **9.2.12.2.** Incident and Escalation management processes.
- **9.2.12.3.** Daily standard operating procedures.
- **9.2.12.4.** Training procedures and material.
- **9.2.12.5.** Reporting metrics and continuous improvement procedures.
- **9.2.12.6.** Data retention and disposal procedures.
- **9.2.12.7.** BCP and DR plan and procedures for SOC
- **9.2.12.8.** Security Patch Management procedure

9.2.13. The bidder should document all the above processes and are to be made available to the bank. The documents are to be reviewed as per the Bank's requirement.

9.2.14. The technical bid should include an overview of the processes mentioned above.

- **9.2.14.1.** Implement necessary security measures for ensuring the information security of the proposed SOC.

9.2.14.2. Develop Escalation Matrix in order to handle Information Security Incidents efficiently.

9.2.14.3. Provide necessary documentation for the operation, integration, customization, and training of each of the solutions in scope.

9.3. Monitoring

The bidder is required to provide the resource count for the operations of the SOC as a part of the response to this RFP and specify the same in the Annexure 6 Resource plan matrix. The bidder should monitor SOC activities and events from each solution and devices already present in Canara Bank's environment on a 24x7x365 basis and suggest/ take appropriate action on an on-going basis. Minimum two resources should be available in any shift from SI.

9.4. Continuous Improvement

Improve the policies configured on an on-going basis to reduce the occurrence of false positives.

9.5. Solution Acceptance

The Bank/appointed consultant in coordination with the bidder shall conduct an Acceptance test wherein the bidder has to demonstrate the implementation of the solution as per the technical requirements (Annexure 2) of this RFP. The bidder shall submit the detailed reports of the test outcomes to Canara Bank.

9.6. SLA Compliance

The bidder shall ensure compliance with SLAs as defined in the RFP.

9.7. Business Continuity

The bidder is responsible for defining a DR/BCP plan for the SOC operations and also ensure that periodic tests are conducted as per the testing requirements of Canara Bank.

9.8. Period of Contract

9.8.1. Bidder is required to provide the services for a period of 6 years.

9.8.2. Post completion of the contract/ or in the event of early termination, the bidder is expected to provide support for transition of the services to the nominated members of Canara Bank (or) to a third party nominated by the bank.

9.8.3. The Bidder is required to provide the warranty/ AMC services at Bank's DC/DR/DIT and other locations for which tools are procured or where tools are deployed, directly or through their OEM representatives at all locations of Canara bank.

9.8.4. The bidders are expected to provide technical and commercial proposals in accordance with the terms and conditions contained herein. Evaluation criteria, evaluation of the responses to the RFP and subsequent selection of the successful bidder shall be as per the process defined in this RFP. Their decision shall be final and no correspondence about the decision shall be entertained.

B. BID PROCESS

10. Clarification to RFP and Pre-Bid Queries:

10.1. The bidder should carefully examine and understand the specifications, terms and conditions of the RFP and may seek clarifications, if required. The bidders in all such cases should seek clarification in writing in the same serial order as that of the RFP by mentioning the relevant page number and clause number of the RFP as per format provided under Appendix-F.

10.2. All communications regarding points requiring clarifications and any doubts shall be given in writing to the Deputy General Manager, Canara Bank, DIT Wing, HO(Annex), 14 MG Road, Naveen Complex, Bengaluru-01 or an email can be sent to hoditapm@canarabank.com by the intending bidders before **03:00 PM on 05/06/2017 (Monday).**

10.3. No queries will be entertained from the bidders after the above date and time.

10.4. The Bank will consolidate all the written queries and any further queries during the pre-bid meeting and the replies for the queries shall be made available in the Bank's website (www.canarabank.com) and no individual correspondence shall be made. The clarification of the Bank in response to the queries raised by the bidder/s, and any other clarification/amendments/corrigendum furnished thereof will become part and parcel of the RFP and it will be binding on the bidders.

10.5. No oral or individual consultation will be entertained.

11. Pre-Bid meeting:

11.1. A pre-bid meeting of the intending bidders will be held as scheduled below to clarify any point/doubt raised by them in respect of this RFP.

Date	Day	Time	Venue
07/06/2017	Wednesday	3:00 PM	Canara Bank, Second Floor, Conference Hall, DIT Wing-HO (Annex), Naveen Complex, 14 M G Road, Bengaluru 560001.

No separate communication will be sent for this meeting. If the meeting date is declared as a holiday under NI Act by the Government subsequent to issuance of RFP, the next working day will be deemed to be the pre-bid meeting day. Authorized representatives of interested bidders shall be present during the scheduled time. In this connection, Bank will allow maximum of Two(2) representatives from each Bidder to participate in the pre-bid meeting.

11.2. Bank has the discretion to consider any other queries raised by the bidder's representative during the pre-bid meeting.

11.3. Bank will have liberty to invite its technical consultant or any outside agency, wherever necessary, to be present in the pre-bid meeting to reply to the technical queries of the Bidders in the meeting.

11.4. The Bank will consolidate all the written queries and any further queries during the pre-bid meeting and the replies for the queries shall be made available in the Bank's website (www.canarabank.com) and no individual correspondence shall be made. The clarification of the Bank in response to the queries raised by the bidder/s, and any other clarification/amendments/corrigendum furnished thereof will become part and parcel of the RFP and it will be binding on the bidders.

11.5. Non reply to any of the queries raised by the vendors during pre-bid Meeting shall not be considered as acceptance of the query/issue by the Bank.

12. Amendment to Bidding Document:

12.1. At any time prior to deadline for submission of Bids, the Bank, for any reason, whether, at its own initiative or in response to a clarification requested by prospective bidder, may modify the bidding document, by amendment.

12.2. Notification of amendments will be made available on the Bank's website only (i.e. www.canarabank.com) and will be binding on all bidders and no separate communication will be issued in this regard.

12.3. In order to allow prospective bidders reasonable time in which to take the amendment into account in preparing their bids, the Bank, at its discretion, may extend the deadline for a reasonable period as decided by the Bank for submission of Bids.

13. Bid System Offer

This is two bid system which has following 3 (Three) parts:

The bids shall be submitted with the following documents in the same sequence without which the tender will be summarily rejected. All the pages in the respective bids should be serially numbered and signed by the authorized person.

The technical and commercial bids should be submitted in "Hard copy" and "Soft Copy". The soft copy should be in a CD/DVD with the name of the system integrator and the type ("Conformity to Eligibility Criteria", "Technical Proposal" and "Commercial Bid") clearly indicated on the CD/DVD. The CD/DVD should be included in the respective sealed cover.

In case of any discrepancy between the "hard copy" and "Soft Copy" documents, the signed "hard Copy" shall be considered final.

13.1. Part A- Conformity to Eligibility Criteria: Indicating their compliance to Eligibility Criteria. The format for submission of Conformity to Eligibility Criteria is as per **Appendix-A.**

13.2. Part B-Technical Proposal: Indicating the response to the Technical specification of **Setting up Security Operations Centre in Canara Bank.** The format for submission of Technical Proposal is as per **Appendix-B.**

13.3. Part C-Commercial Bid: furnishing all relevant information as required as per Commercial Bill of Material as per **Annexure-5.** The format for submission of Commercial Bid is as per **Appendix-C.**

14. Preparation of Bids:

14.1. The Bid shall be typed or written in English language with font size of 12 in indelible ink and shall be signed by the Bidder or a person or persons duly authorized to bind the Bidder to the Contract. The person or persons signing the Bids shall affix signature in all pages of the Bids, except for un-amended printed literature.

14.1.1. The three parts as stated above, should be placed in three separate envelopes superscripted with 'Conformity to Eligibility Criteria', 'Technical Proposal' and 'Commercial Bid' respectively and properly closed and sealed. Thereafter, all the three envelop shall be placed inside another envelope and properly closed and sealed. The final envelope should be superscripted as **"Offer for Selection of Security System Integrator to set up of Information Security Operations Centre in Canara Bank in response to RFP 05/2017-18 dated 26/05/2017"** (includes separately sealed 'Conformity to Eligibility Criteria', 'Technical Proposal' and 'Commercial Bid') on the top of the envelope. All the envelopes shall bear the

name and complete postal address of the bidder as well as the addressee, namely the Deputy General Manager, Canara Bank, AP&M Group, DIT Wing, First Floor, Naveen Complex, 14 M G Road, Bengaluru - 560001.

14.1.2. All the pages of Bid including Brochures should be made in an organized, structured, and neat manner. Brochures / leaflets etc. should not be submitted in loose form. All the pages of the submitted bids should be paginated with Name, Seal and Signature of the Authorized Signatory. Bids with erasing / overwriting / cutting without authentication may be liable for rejection. Authorization letter for signing the Bid documents duly signed by Company's Authorized signatory should be submitted.

14.1.3. All the envelopes shall bear the name and complete postal address of the Bidder and authority to whom the Bid is submitted.

14.2. Part A- Conformity to Eligibility Criteria:

14.2.1. Before submitting the bid, the bidders should ensure that they confirm to the eligibility criteria as stated in **Annexure-1** of RFP. Only after satisfying themselves of the eligibility, the Offer should be submitted.

14.2.2. The Conformity to Eligibility Criteria as per **Annexure-1** among others must contain Demand Draft towards the Application Money as per the **Clause15,** Singed Pre Contract Integrity Pact as per **Appendix-G** and EMD/ Bank Guarantee in lieu of EMD as per **Appendix-D** of this document. The Conformity to Eligibility Criteria should be complete in all respects and contain all information sought for, as per **Appendix-A.**

14.2.3. The Placement of Application Money, EMD and Integrity Pact in other than **Part A-Conformity to Eligibility Criteria** will make the bid liable for rejection.

14.2.4. After ensuring the above, it shall be placed inside a separate Envelope and sealed and superscripted on the top of the cover as **"PART A-Conformity to Eligibility Criteria** for **RFP 05/2017-18 dated 26/05/2017 for Selection of Security System Integrator to set up of Information Security Operations Centre in Canara Bank".**

14.3. Part B-Technical Proposal:

14.3.1. Technical Proposal should be submitted as per the format in **Appendix-B.** Relevant technical details and documentation should be provided along with Technical Proposal.

14.3.2. It is mandatory to provide the technical details of the Solution required by the bank in the exact format of **Annexure-2** of this tender.

14.3.3. The offer may not be evaluated and may be rejected by the Bank without any further reference in case of non-adherence to the format or partial submission of technical information as per the format given in the offer.

14.3.4. If any part of the technical specification offered by the bidder is different from the specifications sought in our RFP, the bidder has to substantiate the same in detail the reason for their quoting a different specification than what is sought for, like higher version or non-availability of the specifications quoted by us, invariably to process the technical offer.

14.3.5. The Bank shall not allow / permit changes in the technical specifications once it is submitted.

14.3.6. The relevant product information, brand, and model number offered, printed product brochure, technical specification sheets etc. should be submitted along with the Offer in the annexure 4 Technical Bill of Materials. Failure to submit this information along with the offer may result in disqualification.

14.3.7. The Technical Proposal should be complete in all respects and contain all information sought for, as per **Appendix-B. Masked Bill of Material must be attached in Technical Offer and should not contain any price information.** The Part B-Technical Proposal should be complete and should cover all products and services. Technical Proposal without masked Bill of Materials will be liable for rejection.

14.3.8. Masked Bill of Material which is not as per below instruction will make Bid liable for rejection:

14.3.8.1. Should be replica of Bill of Material except that it should not contain any price information (with Prices masked).

14.3.8.2. It should not provide any price information like, unit price, tax percentage, tax amount, AMC/ATS charges, Implementation Charges etc.

14.3.9. After ensuring the above, it shall be placed inside a separate Envelope and sealed and superscripted on the top of the cover as **"PART B-Technical Proposal for RFP 05/2017-18 dated 26/05/2017 for Selection of Security System Integrator to set up of Information Security Operations Centre in Canara Bank".**

14.4. <u>Part C-Commercial Bid:</u>

14.4.1. Commercial Bid should be submitted as per the instruction in **Appendix-C.**

14.4.2. Commercial Bid shall be submitted as per Bill of Material and other terms and conditions of RFP on prices. Bill of Material should give all relevant price information as per **Annexure-5.** Any deviations from the Bill of Material / non submission of prices as per the format shall make the bid liable for rejection.

14.4.3. Under no circumstances the Bill of Material should be kept in Part-A (i.e. Conformity to Eligibility Criteria) or Part B (i.e. Technical Proposal) Covers. **The placement of Bill of Material in Part A (i.e. Conformity to Eligibility Criteria) or Part B (i.e. Technical Proposal) covers will make bid liable for rejection.**

14.4.4. The Bill of Material must be attached in Technical Proposal as well as Commercial Bid. The format will be identical for both Technical Proposal and Commercial Bid, **except that the Technical Proposal should not contain any price information (with Prices masked).** Any change in the Bill of Material format may render the bid liable for rejection.

14.4.5. Bidder must take care in filling price information in the Commercial Offer, to ensure that there are no typographical or arithmetic errors. All fields must be filled up correctly.

14.4.6. Any change in the Bill of Material format may render the bid liable for rejection. The Commercial Bids that are incomplete or conditional are liable to be rejected.

14.4.7. The Bidder should indicate the individual taxes, and its applicable rate along with the estimated tax amounts to be paid by the Bank.

14.4.8. If any of the deliverable product, mainly, Hardware, software, Service/Support etc. has both VAT and Service Tax, the bidder has to indicate the Goods component with percentage of VAT and Service Component with service Tax involved. The Goods Component + Service Component should be limited to 100% of the Cost Price. For example, if Goods Component is 60% then, the Service Component cannot be more than 40%.

14.4.9. After ensuring the above, it shall be placed inside a separate Envelope and sealed and superscribed on the top of the cover as **"PART C-Commercial Bid for RFP 05/2017-18 dated 26/05/2017 for Selection of Security System Integrator to set up of Information Security Operations Centre in Canara Bank"**.

15. Application Money:

15.1. This document can be downloaded from Bank's website http://canarabank.com/english/announcements/tenders. In that event, the bidders should pay the Application Fee of **Rs. 25,000/-(non-refundable)** for tender document by means of DD drawn on any scheduled Commercial Bank in favor of Canara Bank, payable at Bengaluru and submit the same along with **Part A-Conformity to Eligibility Criteria.**

15.2. Submission of the Application Money in other than "Part-A-Conformity to the Eligibility Criteria" is liable to be rejected on grounds of non-payment of the Application Money.

15.3. The Bidder shall bear all costs associated with the preparation and submission of the Bid and Bank will not be responsible for the costs, regardless of the conduct or outcome of the bidding process. The Bank is not liable for any cost incurred by the Bidder in replying to this RFP. It is also clarified that no binding relationship will exist between any of the respondents and the Bank until the execution of the contract.

16. Earnest Money Deposit (EMD)/Bank Guarantee In Lieu Of EMD:

16.1. The bidder shall furnish Non interest earning Earnest Money Deposit (EMD) of **Rs.75,00,000/- (Rupees Seventy Five Lakhs Only)**by way of Demand Draft drawn on any Scheduled Commercial Bank In India in favour of Canara Bank, payable at Bengaluru and should be kept along with the **Part-A-Conformity to Eligibility Criteria.**

16.2. In Case the EMD is submitted in the form of Bank Guarantee the same should be valid for the minimum period of 6 months with additional claim period of 3 months from the last date for submission of offer. Bank at its discretion can demand for extension for the validity of EMD. The format for submission of EMD in the form of Bank Guarantee is as per **Appendix-D**.

16.3. Submission of EMD in other than Part A-Conformity to Eligibility Criteria Envelope is liable to be rejected on grounds of non-submission of EMD.

16.4. The EMD of the Bidders not qualified under Technical Proposal will be returned within 15 days after opening the Commercial Bid of the Technically Qualified Bidders. The EMD of Technically Qualified bidders will be returned upon the selected bidder accepting the order and furnishing the Performance Bank Guarantee.

16.5. The EMD may be forfeited/ Bank Guarantee may be invoked:

16.5.1. If the bidder withdraws or amends the bid during the period of bid validity specified in this document.

16.5.2. If the selected bidder fails to accept the purchase order within 7 days or fails to sign the contract or fails to furnish performance guarantee in accordance with the terms of the RFP.