

**Request for Proposal (RFP)**  
**for**  
**Information System Audit**  
**of**

**(A) Audit of Information Security Architecture & Implementation  
of Information Security Policy**

**(B) IS Audit of key IT Systems and resources**

**a) Network Management & Security Audit**

**b) Data Centre - CBS Operations**

**c) Disaster Recovery Site – BCP**

**d) IT Products**

Section – I

## **1. Introduction and Disclaimer**

This Request for Proposal document (“**RFP**”) has been prepared solely to enable Dena Bank (“**Bank**”) in the selection of suitable organisation (Service Provider – SP) to tender for assisting the Bank in conducting IS Audit

The RFP document is not a recommendation, offer or invitation to enter into a contract, agreement or other arrangement in respect of the services.

## **2. Information Provided**

The RFP document contains statements derived from information that is believed to be reliable at the date obtained but does not purport to provide all of the information that may be necessary or desirable to enable an intending contracting party to determine whether or not to enter into a contract or arrangement with Bank in relation to the provision of services. Neither Bank nor any of its employees, agents, contractors, or advisers gives any representation or warranty, express or implied as to the accuracy or completeness of any information or statement given or made in this RFP document. Neither Bank nor any of its employees, agents, contractors, or advisers has carried out or will carry out an independent audit or verification or due diligence exercise in relation to the contents of any part of the RFP document.

## **3. for Respondent Only**

The RFP document is intended solely for the information of the party to whom it is issued (“the **Recipient**” or “the **Respondent**”) and no other person or organisation.

## **4. Confidentiality**

The RFP document is confidential and is not to be reproduced, transmitted, or made available by the Recipient to any other party. The RFP document is provided to the Recipient on the basis of the undertaking of confidentiality given by the Recipient to Bank. Bank may update or revise the RFP document or any part of it. The Recipient acknowledges that any such revised or amended document is received subject to the same terms and conditions as this original and subject to the same confidentiality undertaking.

The Recipient will not disclose or discuss the contents of the RFP document with any officer, employee, consultant, director, agent, or other person associated or affiliated in any way with Bank or any of its customers, suppliers, or agents without the prior written consent of Bank.

## **5. Disclaimer**

Subject to any law to the contrary, and to the maximum extent permitted by law, Bank and its officers, employees, contractors, agents, and advisers disclaim all liability from any loss or damage (whether foreseeable or not) suffered by any person acting on or refraining from acting because of any information, including forecasts, statements, estimates, or projections contained in this RFP document or conduct ancillary to it whether or not the loss or damage arises in connection with any negligence, omission, default, lack of care or misrepresentation on the part of Bank or any of its officers, employees, contractors, agents, or advisers.

## **6. Costs Borne by Respondents**

All costs and expenses incurred by Recipients / Respondents in any way associated with the development, preparation, and submission of responses, including but not limited to attendance at

meetings, discussions, demonstrations, etc. and providing any additional information required by Bank, will be borne entirely and exclusively by the Recipient / Respondent.

## **7. No Legal Relationship**

No binding legal relationship will exist between any of the Recipients / Respondents and Bank until execution of a contractual agreement.

## **8. Recipient Obligation to Inform Itself**

The Recipient must conduct its own investigation and analysis regarding any information contained in the RFP document and the meaning and impact of that information.

## **9. Evaluation of Offers**

Each Recipient acknowledges and accepts that Bank may, in its absolute discretion, apply whatever criteria it deems appropriate in the selection of organisations, not limited to those selection criteria set out in this RFP document.

The RFP document will not be construed as any contract or arrangement which may result from the issue of this RFP document or any investigation or review carried out by a Recipient. The Recipient acknowledges by submitting its response to this RFP document that it has not relied on any information, representation, or warranty given in this RFP document.

## **10. Errors and Omissions**

Each Recipient should notify Bank of any error, omission, or discrepancy found in this RFP document.

## **11. Acceptance of Terms**

A Recipient will, by responding to Bank RFP, be deemed to have accepted the terms as stated above from Para 1 through Para 10.

## **12. Submission of Bids**

Two (2) paper copies and one (1) electronic copy (Microsoft XP Word / Microsoft Power Point and Excel, on CD ROM) of all submissions must be supplied to and addressed to "Bank's Evaluation Office" at :

**The Asst. General Manager,  
Inspection and Internal Audit  
Dena Bank H.O. 17, Horniman Circle, Fort,  
Mumbai – 400 001.**

### **12.1 Submission will be valid if :**

Application Money is paid before pre-bid meeting.

Copies of the RFP are submitted before the schedule closing time.

Submission is not by Fax transmission.

Bids are submitted in two separate sealed envelopes with separate marking "Technical Proposal" & "Commercial Proposal"

All separate copies of RFP and attachments must be provided in a **sealed** envelope or satchet “.

Soft copies of all annexures must be provided on a CD

EMD is enclosed only in the “Technical Proposal”

***Only One Submission Permitted***

Only one submission of tender by each SP will be permitted. In case of partnerships / consortium, only one submission is permitted through the SP.

## **12.2 Registration of RFP**

Registration will be effected upon Bank receiving the RFP response in the above manner (Para 12). The registration must contain all documents, information, and details required by this RFP. If the submission to this RFP does not include all the information required or is incomplete or submission is through Fax mode, the RFP is liable to be rejected.

All submissions, including any Banking documents, will become the property of Bank. Recipients shall be deemed to license, and grant all rights to, Bank to reproduce the whole or any portion of their submission for the purpose of evaluation, to disclose the contents of the submission to other Recipients who have registered a submission and to disclose and/or use the contents of the submission as the basis for any resulting RFP process, notwithstanding any copyright or other intellectual property right that may subsist in the submission or Banking documents.

## **12.3 Late RFP Policy**

Respondents are to provide detailed evidence to substantiate the reasons for a late RFP submission.

RFPs lodged after the deadline for lodgment of RFPs may be registered by Bank and may be considered and evaluated by the evaluation team at the absolute discretion of Bank. It should be clearly noted that Bank has no obligation to accept or act on any reason for a late submitted response to RFP.

Bank has no liability to any person who lodges a late RFP for any reason whatsoever, including RFPs taken to be late only because of another condition of responding.

## **12.4. Tender Validity Period**

The bids will remain valid for a period of at least six (6) months from the date of opening the technical bids.

## **12.5. Requests for Information**

Recipients are required to direct all communications related to this RFP through the Nominated Point of Contact person i.e.

**The Asst. General Manager,  
Inspection and Internal Audit  
Dena Bank H.O. 17, Horniman Circle, Fort,  
Mumbai – 400 001.  
Email ID: [insp-audit@denabank.co.in](mailto:insp-audit@denabank.co.in)**

All questions relating to the RFP, technical or otherwise, must be in writing only to the Nominated Point of Contact.

Bank will not answer any communication initiated by Respondents later than five business days prior to the due date for bids submission. However, Bank may in its absolute discretion seek, but under no obligation to seek, additional information or material from any Respondents after the tender closes and all such information and material provided must be taken to form part of that Respondent's response.

Respondents should invariably provide details of their email address(es) as responses to queries will only be provided to the Respondent via email.

If Bank in its absolute discretion deems that the originator of the question will gain an advantage by a response to a question, then Bank reserves the right to communicate such response to all Respondents.

Bank may in its absolute discretion engage in discussion or negotiation with any Respondent (or simultaneously with more than one Respondent) after the tender closes to improve or clarify any response.

### **13. Notification**

Bank will notify the Respondents in writing as soon as practicable about the outcome of the RFP evaluation process, including whether the Respondent's RFP response has been accepted or rejected. Bank is not obliged to provide any reasons for any such acceptance or rejection.

### **14. Disqualification**

Any form of canvassing/lobbying/influence/query regarding short listing, status etc will be a disqualification.

### **15. Process**

Selection of a successful SP will involve a 8 stages approach. The approach follows the Indian Government's Central Vigilance Commission (CVC) guidelines.

#### **1. Issue of Tender Notification**

This RFP is made available at the Bank's web site [www.denabank.com](http://www.denabank.com) under tenders. And also send by e-mail/post to the current CERT-In empanelled organizations.

#### **2. Pre-bid meeting**

The pre-bid meeting will be organized at the **Bank's Evaluation Office** on the scheduled date. All the queries or clarifications of the bidders shall be answered by the Bank. Those who are interested to attend the meeting should bring the application money on the same day. The reply or any further changes in the RFP shall be communicated during the meeting OR sent to the participants only. However those who could not attend the meeting but if they have submitted the application money before the pre-bid meeting shall also be communicated the outcome of the pre-bid meeting.

#### **3. Submission of Bids**

#### **4. Technical bids Evaluation**

#### **5. Commercial bids comparison**

#### **6. Negotiation with the final bidder**

7. Issuance of letter of appointment (LoA)
8. Acceptance of the LoA

### **15.1. Process Timeframe**

The following is an indicative timeframe for the overall selection process. Bank reserves the right to vary this timeframe at its absolute and sole discretion should the need arise. Changes to the timeframe will be relayed to the affected Respondents during the process.

<b>Description</b>	<b>Due Date</b>
Issue Tender Notification	24-10-2008
Pre – bid meeting	07-11-2008
Tender Submission	14-11-2008 before 4 pm
Technical bids opening	14-11-2008 at 5 pm
Technical Evaluation Completion	21-11-2008
Commercial evaluation & Issuance of LoA	28-11-2008
Acceptance of LoA	05-12-08
Submission of all reports and Deliverables	30-01-09

\* All dates mentioned above are tentative dates and the bidder acknowledges that it cannot hold the Bank responsible for breach of any of the dates

**Section – II**



## **1. Bank – the Bank**

### ***Introduction***

Dena Bank was founded on 26th May, 1938 by the family of Devkaran Nanjee under the name Devkaran Nanjee Banking Company Ltd.

It became a Public Ltd. Company in December 1939 and later the name was changed to Dena Bank Ltd.

In July 1969, Dena Bank Ltd. along with 13 other major banks was nationalized and is now a Public Sector Bank constituted under the Banking Companies (Acquisition & Transfer of Undertakings) Act, 1970.

The financial performance of the bank is enumerated below:

The capital stood at Rs. 286.82 crores with total reserves 1279.70 crores as of March'08. The deposits stood at Rs. 33943.18 crores and total advances stood at 23381.16 crores as of March'08. The gross profit was at Rs. 686.44 crores and net profit was at Rs. 359.79 crores.

The Bank is having a three tier organizational structure comprising of Branches, Regional Offices, Head Office with a network of 1160 Branches spread across the country with presence in almost all major states and Union Territories. We have specialized branches that caters to various customer segments viz. Industrial Finance Branch, Overseas Business Branches, Asset Recovery Branches, SSI Branch, International Banking Branch, Capital Market Branch, Service Branches and Satellite Offices.

### ***Bank's Mission***

Dena Bank will provide its customers – premier financial services of great value, staff - positive work environment and opportunity for growth and achievement and shareholders – superior financial returns, community – economic growth.

The Bank has chosen Finacle Software of M/s.Infosys Ltd., as the Core Banking Solution and the CBS project is implemented and supported by M/s. Wipro. The bank's Dept. of IT, HO as well as the Primary Data Centre are located at Mumbai. The D/R Data Centre are located at Bangalore.

### **Classification & Category of Branches**

**Category wise region-wise distribution of branches:**

**Table # 1**

<b>Sr. No.</b>	<b>Region</b>	<b>Metropolitan</b>	<b>Urban</b>	<b>Semi Urban</b>	<b>Rural</b>	<b>Total</b>
	<b>Ahmadabad</b>	36	0	5	12	<b>53</b>
	<b>Bhavnagar</b>	0	6	19	28	<b>53</b>
	<b>Bhuj</b>	0	11	25	36	<b>72</b>
	<b>Gandhinagar</b>	0	0	11	55	<b>66</b>
	<b>Mehsana</b>	0	0	16	45	<b>61</b>
	<b>Rajkot</b>	0	17	21	17	<b>55</b>
	<b>Surat</b>	0	18	42	70	<b>130</b>
	<b>Vadodara</b>	0	19	24	30	<b>73</b>
	<b>Mumbai City</b>	28	0	0	0	<b>28</b>
	<b>Mumbai Suburb</b>	43	0	0	0	<b>43</b>
	<b>Nashik</b>	0	19	16	22	<b>57</b>
	<b>Pune</b>	10	12	9	22	<b>53</b>
	<b>Thane</b>	0	13	17	30	<b>60</b>
	<b>Bangalore</b>	24	13	3	5	<b>45</b>
	<b>Bhopal</b>	0	23	9	3	<b>35</b>
	<b>Kolkatta</b>	21	22	7	3	<b>53</b>
	<b>Chennai</b>	0	28	3	1	<b>32</b>
	<b>Lucknow</b>	2	33	6	8	<b>49</b>
	<b>New Delhi</b>	26	37	5	4	<b>72</b>
	<b>Raipur</b>	0	11	8	41	<b>60</b>
<b><u>BRANCHES UNDER HEAD OFFICE</u></b>						
1) I.F.B. H.O. MUMBAI						1
2) ASSET RECOVERY BRANCH, MUMBAI						1
3) INTERNATIONAL BANKING BRANCH, MUMBAI						1
4) CORPORATE BUSINESS BRANCH, BKC, MUMBAI						1

### **Products offered**

#### **Products and services offered by the Bank**

The bank has a rich assortment of Deposits, Loans, Remittances, Bills, Foreign Exchange Business and other fee based products.

### **Deposit Products**

Current Deposits

Savings Bank Deposits

Flexi deposits

Capital Gains Deposits

NRO/NRE Deposits

Savifix

SDR

FCNR

Capital gains

1) Recurring deposits

**Working Capital Finance**

1) Cash credit accounts against stocks and book debts (CCH)

2) Packing Credit

3) Export Finance

**Term Lending**

1) Short term

2) Medium Term

3) Long Term

4) Consortium/Syndicated Loans

**Trade Finance – non-fund based**

1) Letter of credit

2) Bank Guarantee

3) Deferred Payment Guarantee

**Bills Business**

1) Collection of bills and cheques - Inward and outward

2) Purchase/Discounting of sales/drawee bills (clean and documentary) / Cheques

3) Bills Related Advances

**Retail Loans – Dena Finmart**

1) Dena Niwas

2) Dena Mortgage

3) Dena Rent

4) Dena Senior Citizen

5) Dena Trade Finance

6) Dena Vidya Laxmi

7) Dena Auto Finance

8) Dena Suvidha

9) Dena Consumer Durable

**Industrial/Corporate Loans**

### **Remittances**

- 1) Demand Draft – Issue/payment
- 2) Banker's Cheque/Pay Orders – Issue/Payment
- 3) Mail Transfer – Issue / payment
- 4) Telegraphic Transfer – Issue / Payment
- 5) Inter-branch Transactions – originating/responding
- 6) Funds Remittance – (Inter Branch and Inter Bank Remittance) – Inward/outward

### **Government Business**

- 1) Pension payments (State / Central / Railways)
- 2) Direct Tax collection
- 3) Relief Bonds
- 4) Tax Collection

### **Specialised Activities**

- 1) Dealings Operation

### **Miscellaneous Services**

- 1) Locker Services
- 2) Dividend/Interest/Refund Warrants
- 3) Agency Arrangement with other Banks
- 4) Bancassurance

### ***CBS and Other Details***

#### **1.11.1 CBS**

In June, 2006, Bank has started the process of CBS implementation for its 850+ branches. First branch was migrated to CBS on 12<sup>th</sup> March 2007. As of 18/10/2008, **330** branches have been brought under the CBS platform covering **124 centres / 20 regions(Excluding HO) / 24 states**. Of these, 52 branches (all new branches opened after 12.03.2007) and 278 branches have migrated from their existing TBC software (165 Cheqmate, 104 Virmati and 9 Service branches) .

#### **1.11.2 Networking**

Bank has set up its own network named as “**DENANET**” using 651 Leased Lines, 336 ISDN lines , 26 VSATs and 598 Dial-up lines connecting 1068 branches, 36 administrative offices spread over 300 centers. This network supports Bank's inter – connected ATMs seamlessly. Critical applications like Any Branch Banking (ABB) and Real Time Gross Settlement (RTGS) transactions and other functions like sending OLTAS data to OLTAS Nodal/Link branches, the corporate e-mail service, MIS data transfer between branches, Regional Offices & Corporate Office and remote support to Branches / RO are enabled by Denanet.

### **1.11.3 ATMs**

**As on March, 2008**, a total of 316 ATMs have been installed all over the country. Out of these ATMs, 243 are Onsite and 73 are Offsite covering 142 centers. Besides this, Bank has ATM sharing arrangement with Corporation Bank and **CashTree** group of banks (BOI, United Bank, Syndicate Bank, Indian Bank, Union bank, BOM, IOB, Bank of Rajasthan, Karnataka bank and Yes Bank etc)

Bank has also joined **Cashnet** group Banks that includes IDBI Bank, Citibank, Standard Chartered, Centurion Bank, UTI Bank, Deutsche Bank, ING Vysya Bank, Development Credit Bank, The Dhanalakshmi Bank Ltd., HDFC and also with Corporation Bank for mutual sharing of ATMs and also tied up with SBI & NFS group of Banks for mutual sharing of ATM.

**Section – III**

## 1. Current RFP Objectives:

### 2.1 Audit Objectives

The Bank wishes to appoint competent SP for conducting an IS Audit of its IT Security architecture and Information System resources and infrastructure with the major objectives of evaluation of internal system and control for

Safeguarding of Information System Assets/Resources  
Maintenance of Data Integrity, Reliability and Confidentiality  
Maintenance System Effectiveness.  
Ensuring System Efficiency.

The SP will be responsible as per the scope and timelines outlined below.

### 2.2. Audit Approaches

Information Systems Audit approach includes the following

Auditing around the computer  
Auditing through the computer  
Auditing with the computer

Through preparation of IS audit checklists based on globally accepted standards and RBI guidelines/circulars.

Based on the audit findings risk assessment to be classified as Low, Medium, High, Very High and Extremely high in each specific audit areas.

### 2.3 Audit Methodology

The IS audit work will include manual procedures, computer assisted procedures and fully automated procedures, depending on the chosen audit approach.

### 2.4 Auditors:

Audit should be carried out by CERT-In empanelled audit firm by persons having **CISA/ DISA /CISSP / CISM / GIAC(SANS)** qualifications with adequate experience in the audit areas given below.

### 2.5 Audit Scope:

A description of the envisaged scope is enumerated in brief as under and in detail in Annexure - A. However, the Bank reserves its right to change the scope of the RFP considering the size and variety of the requirements and the changing business conditions. The Bank groups the entire proposed audits into five **major AREAS** as under -

(A) Audit of Information Security Architecture & Implementation of Information Security Policy (Area-1)

(B) IS Audit of key IT Systems and resources

a. Network Management & Security Audit (Area-2)

b.Data Centre - CBS Operations (Area-3)

c.Disaster Recovery Site – BCP (Area-4)

d.IT Products (Area-5)

Based on the contents of the RFP, the selected SP shall be required to independently arrive at Audit Methodology, based on globally acceptable standards and best practices

The Bank expressly stipulates that the SP's selection under this RFP is on the understanding that this RFP contains only the principal provisions for the entire audit assignment. The SP shall be required to undertake to perform all such tasks, render requisite services and make available such resources as may be required for the successful completion of the entire audit assignment at no additional cost to the Bank.

## **2.6 Audit Findings & Reports:**

Risk analysis along with Risk Matrix with scoring model should be submitted as part of audit findings.

Deliverables Under the IS Audit – the SP will deliver detailed reports as below:

The following reports are an indicative that should be covered for the area-wise auditing-

- 1) IS Audit (Technical & Process) Report of all the areas covering the objectives, efficiency and effectiveness
- 2) Presentation to the Top Management of the findings of the Reports
- 3) Risk Analysis Report
- 4) Recommendations for Risk Mitigation
- 5) Gap analysis and recommendation for mitigation
- 6) The check list with guidelines for the subsequent audit (hard & soft copies)

The report findings should cover all the areas separately mentioned in the scope.

## **2.7 Duration of Audit:**

The entire audit should be completed within 2 ½ months from the date of letter of appointment.

## **2.8 Pre-Qualification Criteria**

The SP is required to meet the following minimum eligibility criteria and provide adequate documentary evidence for each of the criteria stipulated below:

- 2.8.1. The SP should be in existence for a period of at least 3 years
- 2.8.2. The SP should have a minimum total turnover (revenue from IS audit) of Rs. 100 lacs in the last two years
- 2.8.3. The SP should be a profit making company in the last 2 years
- 2.8.4. The SP should have a current CERT-In (Indian Computer Emergency Response team ) empanelled
- 2.8.5. The SP should have a pool of resources who possess qualifications such as :



CISA/ CISSP/ CCNA/ CISM/ GIAC(SANS),DISA

2.8.6. The SP should have audited at least two audit areas mentioned as above in any scheduled commercial banks having not less than 500 branches in India.

2.8.7. Existing Dena Bank's CBS consultant/supplier is not eligible to participate in the audit.

## **2.9 Earnest Money Deposit**

Subject to compliance of Response Submission Process as elucidated in Section – I, the intending bidders should pay along with bids an Earnest Money Deposit of Rs. 1,00,000/- (Rupees one lakh only). The EMD shall be paid by Demand Draft / Banker's Cheque / Pay Order drawn in favor of 'Dena Bank – A/c Inspection Department' payable at Mumbai. The EMD will not carry any interest.

### **The EMD made by the bidder will be forfeited if :**

- 1 The bidder withdraws his tender before opening of the bids.
- 2 The bidder withdraws his tender after opening of the bids but before acceptance of "Letter of appointment" issued by Bank.
- 3 The selected bidder withdraws his tender before furnishing an unconditional and irrevocable Performance Bank Guarantee.
- 4 The bidder violates any of the provisions of the terms and conditions of this tender specification.
- 5 The EMD will be refunded to
  - The successful bidder, only after furnishing an unconditional and irrevocable Performance Bank Guarantee for 10% of the contract value (valid till the end of assignment period) with 3 (three) months claim period.
  - The unsuccessful bidders, only after acceptance of the "Letter of Appointment" by the selected bidder.

## **2.10 Application Money**

The intending bidders should pay an Application Money of Rs.5,000/- (Rupees five Thousand only). The application money shall be paid by Demand Draft / Banker's Cheque / Pay Order drawn in favor of 'Dena Bank – A/c Inspection Department' payable at Mumbai. The application money is non-refundable.

## **2.11 Submission of Bids (Please refer to Section – I, Para 12)**

The bids shall be in two parts viz. Technical Proposal and Commercial Proposal. Both Technical and Commercial Bids shall be submitted in separate sealed envelopes superscribing **"TECHNICAL PROPOSAL FOR IS AUDIT: TENDER REFERENCE NO. xxx** on top of the envelope containing the technical bid and **"COMMERCIAL PROPOSAL FOR IS AUDIT: TENDER REFERENCE NO. xxx** on top of the envelope containing commercial bid. These two separate sealed envelopes should be put together in the sealed master envelope superscribing **"PROPOSAL for IS AUDIT: TENDER REFERENCE NO. xxx.**

A copy of the Commercial Proposal masking the prices is to be submitted along with the Technical Proposal.

The EMD as mentioned in clause 2.9 is to be submitted along with the Technical Proposal.

Application money of Rs.5,000/- (Rupees five Thousand only) as mentioned as clause 2.10 is to be submitted along with the technical proposal.

The Commercial Proposal shall be submitted as per Annexure B.

The bidder shall submit the Proposals properly filed so that the papers are not loose. The Bidder shall submit the proposal in suitable capacity of the file such that the papers do not bulge out and tear during scrutiny.

The technical proposal shall be organized and submitted as per the following sequence:

Sl.No.	Items	
1	Application fee	Rs.5,000/-
2	EMD (Earnest Money Deposit)	Rs.1,00,000/-
3	Details of business and business background Service Profile & client profile	Annexure – 1
4	Details of experience/knowledge possessed in the areas of Project Planning and management review, Resource Planning, Role and Responsibility definition, Co-ordination across multiple teams, Project risk analysis and containment	Annexure – 2
5	Gross revenue of the bidder (not of the group) Year 2005-06, Year 2006-07, Year 2007-08 CA certified financials	Annexure – 3
6	Net Profit of the bidder (not of the group) Year 2005-06, Year 2006-07, Year 2007-08 CA certified financials	Annexure – 4
7	Details of the similar assignments executed by the bidder in the Banks	Annexure – 5
8	Details of the similar assignments executed by the bidder in other than Banking industry	Annexure – 6
9	Details of lead audit certification from leading certification Bodies	Annexure – 7
10	Details of inputs, infrastructure requirements required by the bidder to execute this assignment.	Annexure – 8
11		
12	Details of the bidder's proposed methodology/approach for providing services to the Bank with specific reference to the scope of work.	Annexure – 9
13	Details of deliverables the bidder proposes with specific reference to the scope of work.	Annexure – 10
14	Masked : Commercial Bid Format	ANNEXURE – B
15	Compliance Certificate	ANNEXURE – C
16	Comments on the Terms & Conditions, Services and Facilities provided	ANNEXURE – D
17	Bidder's profile with the details of past experience	ANNEXURE – E

18	Proposed Team Profile	ANNEXURE – F1
19	Other staff in the SP	ANNEXURE – F2
20	Estimated Effort and Elapsed Time for each audit areas which bidder likes to quote (Annexure – G1 for ISP, Annexure – G2 for NMS, etc.)	ANNEXURE – G1, G2,G3, – G4,G5

All the relevant pages of the proposals (except literatures, datasheets and brochures) are to be numbered and be signed by authorized signatory on behalf of the Bidder. The number should be a unique running serial no. across the entire document.

The bidder has to submit a soft copy of the entire proposal in a CD. It should be noted that in case of any discrepancy in information submitted by the bidder in hard-copy and soft-copy, the hard-copy will be given precedence. However, in case of non-submission of any hard copy document, if the same is found submitted in the soft-copy, Bank reserves right to accept the same at its discretion.

The Bids shall be addressed and submitted to the Banks Evaluation Office.

The bids (arranged as mentioned above) are to be submitted at the above address, marked with the tender number, at the above address before the due date & time as specified. The bid submitted anywhere else is liable to be rejected.

It may be noted that all queries, clarifications, questions etc., relating to this RFP, technical or otherwise, must be in writing only and should be to the nominated point of contact.

Bidders should provide their E-mail address in their queries without fail.

The bidder will submit an undertaking specifying that the bidder has obtained all necessary statutory and obligatory permission to carry out project works, if any.

The proposal should be prepared in English. The e-mail address and phone/fax numbers of the bidder should also be indicated on the sealed cover.

**FORMATS OF BIDS:** The bidders should use the formats prescribed by the Bank in the RFP for submitting both technical and commercial bids.

## **2.12 General Terms and Conditions (Please also refer to Section – I)**

### **2.12.1 Adherence to Terms and Conditions:**

The bidders who wish to submit responses to this RFP should note that they should abide by all the terms and conditions contained in the RFP. If the responses contain any extraneous conditions put in by the respondents, such responses may be disqualified and may not be considered for the selection process.

### **2.12.2 Other terms and conditions:**

1. Bank reserves the right to :
  - 1 Reject any and all responses received in response to the RFP
  - 2 Waive or Change any formalities, irregularities, or inconsistencies in proposal format delivery
  - 3 To negotiate any aspect of proposal with any bidder and negotiate with more than one bidder at a time

- 4 Extend the time for submission of all proposals
- 5 Select the most responsive bidder (in case no bidder satisfies the eligibility criteria in totality)
- 6 Select the next most responsive bidder if negotiations with the bidder of choice fail to result in an agreement within a specified time frame.
- 7 Share the information/ clarifications provided in response to RFP by any bidder, with any other bidder(s) /others, in any form.
- 8 Cancel the RFP/Tender at any stage, without assigning any reason whatsoever.

**3. Substitution of Project Team Members:** During the assignment, the substitution of key staff identified for the assignment will not be allowed unless such substitution becomes unavoidable to overcome the undue delay or that such changes are critical to meet the obligation. In such circumstances, the SP can do so only with the concurrence of the Bank by providing other staff of same level of qualifications and expertise. If the Bank is not satisfied with the substitution, the Bank reserves the right to terminate the contract and recover whatever payments made by the Bank to the SP during the course of this assignment besides claiming an amount, equal to the contract value as liquidated damages. However, the Bank reserves the right to insist the SP to replace any team member with another (with the qualifications and expertise as required by the Bank) during the course of assignment.

**4. Professionalism :** The SP should provide professional, objective and impartial advice at all times and hold the Bank's interests paramount and should observe the highest standard of ethics while executing the assignment.

**5. Adherence to Standards :** The SP should adhere to laws of land and rules, regulations and guidelines prescribed by various regulatory, statutory and Government authorities

6. The Bank reserves the right to conduct an audit/ongoing audit of the consulting services provided by the SP.

7. The Bank reserves the right to ascertain information from the banks and other institutions to which the bidders have rendered their services for execution of similar projects.

## **8. COMMERCIAL BID :**

The prices should be quoted for all areas for the services offered by the SP as per the format enclosed as Annexure – B.

It may be noted that Bank will not pay any amount/expenses / charges / fees / travelling expenses / boarding expenses / lodging expenses / conveyance expenses / out of pocket expenses other than the above "Agreed Professional Fee".

9. The bidder can not change the Project Manager during entire period of execution of the scope unless consented in written by the Bank.

10. The bid should contain the resource planning proposed to be deployed for the project which includes, inter-alia, the number of personnel, skill profile of each personnel, duration etc.

11. The bidder is expected to quote for the prices of the services with the applicable taxes as on the date of bid submission. Any upward / downward revision in the tax rates from the date of the bid submission will be to the account of the Bank

## **12. TERMS OF PAYMENT :**

The SP's fees will be paid in the following manner for each item which is described in the Commercial bid (Annexure - B):

100% on completion of audit, submission of audit findings and reports as per point.no.2.6

## **13. LIQUIDATED DAMAGES (LD) :**

The Bank will impose liquidated damages, of Rs. 5,000/- (Rupees Five thousand only) per week or part thereof, for delay in not adhering to the time schedules (Section-I -15.1).

If the selected Bidder fails to complete the due performance of the contract in accordance to the specifications and conditions agreed during the final contract negotiation, the Bank reserves the right either to cancel the contract or to accept performance already made by the bidder. The Bank reserves the right to recover an amount as deemed reasonable by the Bank as Liquidated Damages for non-performance.

Both the above Liquidated Damages are independent of each other and are applicable separately and concurrently.

LD is not applicable for reasons attributable to the Bank and Force Majeure. However, it is the responsibility of the bidder to prove that the delay is attributed to the Bank and Force Majeure. The bidder shall submit the proof authenticated by the bidder and Bank's official that the delay is attributed to the Bank and Force Majeure along with the bills requesting payment.

## **14.Indemnity :**

The bidder shall indemnify Bank and keep indemnified for against any loss or damage by executing an instrument to the effect on a Non-Judicial stamp paper that Bank may sustain on account of violation of patent, trademarks etc. by the bidder.

## **15.Authorized Signatory :**

The selected bidder shall indicate the authorized signatories who can discuss and correspond with the bank, with regard to the obligations under the contract.

The selected bidder shall submit at the time of signing the contract, a certified copy of the extract of the resolution of their Board, authenticated by Bank , authorizing an official or officials of the Bank or a Power of Attorney copy to discuss, sign agreements/contracts with the Bank. The bidder shall furnish proof of signature identification for above purposes as required by the Bank.

## **16. Applicable Law and Jurisdiction of court :**

The Contract with the selected bidder shall be governed in accordance with the Laws of India for the time being enforced and will be subject to the exclusive jurisdiction of Courts at Mumbai (with the exclusion of all other Courts).

## **17.CANCELLATION OF CONTRACT AND COMPENSATION :**

The Bank reserves the right to cancel the contract of the selected bidder and recover expenditure incurred by the Bank on the following circumstances :

- 1 The selected bidder commits a breach of any of the terms and conditions of the bid/contract.
- 2 The bidder goes into liquidation voluntarily or otherwise.
- 3 An attachment is levied or continues to be levied for a period of 7 days upon effects of the bid.
- 4 The progress regarding execution of the contract, made by the selected bidder is found to be unsatisfactory.
- 5 If deductions on account of liquidated Damages exceeds more than 10% of the total contract price.

After the award of the contract, if the selected bidder does not perform satisfactorily or delays execution of the contract, the Bank reserves the right to get the balance contract executed by another party of its choice by giving one month notice for the same. In this event, the selected bidder is bound to make good the additional expenditure, which the Bank may have to incur to carry out bidding process for the execution of the balance of the contract. This clause is applicable, if for any reason, the contract is cancelled.

The Bank reserves the right to recover any dues payable by the selected bidder from any amount outstanding to the credit of the selected bidder, including the pending bills and/or invoking Bank Guarantee, if any, under this contract or any other contract/order.

## **18.NON PAYMENT OF PROFESSIONAL FEES :**

If any of the items/activities as mentioned in the price bid and as mentioned in annexure G are not taken up by the Bank during the course of this assignment, the Bank will not pay the professional fees quoted by the SP in the Price Bid against such activity/item.

## **19.ASSIGNMENT :**

Neither the contract nor any rights granted under the contract may be sold, leased, assigned, or otherwise transferred, in whole or in part, by the SP, and any such attempted sale, lease, assignment or otherwise transfer shall be void and of no effect without the advance written consent of the Bank.

## **20. Subcontracting :**

The SP shall not subcontract or permit anyone other than its personnel to perform any of the work, service or other performance required of the SP under the contract without the prior written consent of the Bank.

## **21. SP Selection/Evaluation Process:**

The Technical Proposal will be evaluated first for technical suitability. Commercial Proposal shall be opened only for the short-listed bidders who have qualified in the Technical Proposal evaluation.

The evaluation of technical proposals, among other things, will be based on the following parameters and also given the percentage of marks:

Sln.	Parameters	Marks
1	Bidder's overall standing to undertake such assignment (Financial stability)	10%
2	Prior experience of the bidder in undertaking audits in the given areas	50%
3	Proposed Audit Approach & Methodology to be adopted for the audit. IS audit tools to be used, estimated time and report architecture	20%
4	Bidder having Lead Audit certification from leading certification bodies	10%
5	Expertise / Skills available - CISA/ DISA /CISSP / CISM / GIAC(SANS)	10%

Various stages of technical evaluation are presented below:

1. Matching the clear eligibility criteria as indicated under Para 2.8 above
2. Short-listing of the bidders based on the fully matched criteria
3. Paper evaluation based on response
4. Arriving at the final score on technical proposal area of audit wise

At the sole discretion and determination of the Bank, the Bank may add any other relevant criteria for evaluating the proposals received in response to this RFP.

The technical marks cut – off (**TM-CO**) for opening of the commercial bid opening would be 70% (70 marks out of 100) or the area-wise three top scores. SPs scoring below the same would not be considered for commercial bid opening.

In the event only one SP qualifies the Bank will have the right to place the order with the single qualified SP. In the event no SP technically qualifies (i.e. all are below 70%) then the bank may choose to select the SP with the highest score among the area.

**Bank may, at its sole discretion, decide to seek more information from the respondents in order to normalize the bids.** However, respondents will be notified separately, if such normalization exercise as part of the technical evaluation is resorted to.

## **21.1 Commercial Bid Evaluation Criteria**

It may be noted that commercial bids will be subjected to following evaluation process.

Based on the technical evaluation criteria, each bidder will be given certain marks. Only those bidders scoring TM-CO or above in the technical evaluation will be short-listed for commercial evaluation.

### **Computation Methodology for arriving at “Least Price / Least Quote”**

1. “Least Price / Least Quote” will be computed for all bidders having TM-CO or above

2. In the event only one bidder score TM-CO the bank will have the right to open the commercial bid of only that bidder
3. Least price / least quote will be arrived at after taking into account the technical superiority of the bidders based on the table mentioned - below

**Computation of “Least Price / Least Quote”:**

<b>Difference between :</b>	<b>Price Advantage to T1 will be @</b>
T1 (Technically highest) and others is between 5+ to 10 marks	5%
T1 and Others is between 5+ to 10 marks	10%
T1 and Others is greater than 10 marks	25%

Having arrived audit area-wise “Least Price” as above, Bank will prepare a list of bidders based on the “Computed Price Quote” in the order of ascendancy. The bidder whose “Computed Price Quote” is found to be on the top of the list, will be invited for price and contract negotiation.

Bank deserve the right to split the various audit assignments to different SPs if they ranked T1 as well as L1 in that particular area.

Bank reserves the right to negotiate the price with the **finally** short listed bidder before awarding the contract. It may be noted that Bank will not entertain any price negotiations with any other bidder, till the Least Price bidder declines to accept the offer.

The Bank will apply the Technical Evaluation criteria as deemed fit for the purpose of evaluation in consultation with the Committee constituted for this purpose. The evaluation criteria as applied by the Bank will be final and binding and no SP will have the right to challenge or question the criteria applied by the Bank.



**Section-IV**

## **SUPPLEMENTAL TERMS AND CONDITIONS**

### **A. Proprietary and Related Rights**

1. **Bank Property:** All data or information supplied by the Bank to the SP in connection with the services being provided by SP ('the Services') shall remain the property of the Bank or its licensors. All deliverables to the extent prepared by SP hereunder for delivery to the Bank ('the Deliverables') shall be the property of the Bank.
2. **SP Property:** In connection with performing the Services, SP may use certain data, modules, components, designs, utilities, subsets, objects, program listings, tools, models, methodologies, programs, systems, analysis frameworks, leading practices and specifications ('Technical Elements'). Certain Technical Elements were owned or developed by SP prior to, or independently from, its engagement hereunder and are the sole and exclusive property of SP and SP retains all rights thereto, as well as to all modifications, enhancements and derivative works of such Technical Elements created, developed or prepared by SP during the performance of the Services. Certain other Technical Elements consist of third party works and products that SP has acquired the rights to use. In addition SP retains the right to use its knowledge, experience and know-how, including processes, ideas, concepts, and techniques developed in the course of performing the Services, in providing services to other clients. The Bank shall have no rights in the Technical Elements. All working papers prepared by SP in connection with the Services shall remain the property of SP.
3. **Use of Deliverables and Services:** The Deliverables and SP's Services (including any related recommendations and advice) are intended solely for the information and use of the Bank's management, officers, directors and employees and may not be disclosed to any other person without the prior written consent of SP (other than the Bank's external auditors, subject to their agreement that none of the Deliverables, or any portion thereof, shall be further disclosed to any other person or entity except as required by law or professional obligation and that such auditors shall in no event make any claims against SP arising out of or in connection with the Deliverables). If the Deliverables or Services (including any portion, abstract or summary thereof, whether oral or in writing) is disclosed to an unauthorized third party, Bank agrees to indemnify and hold harmless SP, its partners, employees, agents and advisors from and against all claims, causes of action, liabilities, losses, damages, costs, and expenses (including, without limitation, reasonable attorneys' fees) resulting from such disclosure.
4. **Systems:** Unless SP has expressly agreed to do so in writing in this Agreement, the Services do not involve identifying, addressing or correcting any errors or defects in computer systems, other devices, or components thereof ('Systems'), due to imprecise or ambiguous entry, storage, interpretation, processing or reporting of data, including dates, and SP shall have no responsibility or liability for any defect or problem arising out of or related to processing in any Systems. However, during the performance of our engagement, we may become aware of issues with respect to your 'Systems'. These findings will be communicated to you in our individual reports.

### **B. Confidential Information**

1. **Confidentiality:** Except as otherwise expressly provided in the text of the engagement letter, one party receiving Confidential Information, as defined below, in connection with the provision of the

Services shall not disclose such Confidential Information outside of its organization or use it for any purpose other than in connection with the Services. 'Confidential Information' means all information in which a party has rights that is not generally known to the public and that under all the circumstances should reasonably be treated as confidential or proprietary, whether or not the material is specifically marked as confidential. Notwithstanding the foregoing, Confidential Information does not include information that: (i) is, as of the time of its disclosure, or thereafter becomes, part of the public domain through a source other than the receiving party; (ii) was known to the receiving party as of the time of its disclosure; (iii) is independently developed by the receiving party without reference to the Confidential Information; or (iv) is subsequently learned from a third party not known by the receiving party to be subject to an obligation of confidentiality with respect to the information disclosed.

2. Exceptions: Nothing in this Agreement shall limit the ability of a party in possession of the Confidential Information of the other to disclose such Confidential Information, and such party shall have no liability for such disclosure, if such disclosure is: (i) required to be disclosed pursuant to law, regulation, professional responsibility, government authority, duly authorized subpoena or court order whereupon the disclosing party will provide notice to the other party prior to such disclosure; (ii) required to be disclosed to a court or other tribunal in connection with the enforcement of such party's rights under this Agreement; or (iii) is approved for disclosure by the prior written consent of the other party.
3. Survival of Restrictions: The terms of this Section B will survive the termination of this Agreement and will continue in full force and effect for a period of twelve months from the date of such termination or as otherwise required by law or regulation.
4. Conflict of Interest: Subject to confidentiality restrictions set forth herein, SP and its affiliates shall have the right to render similar services to any third parties, even if such parties are in competition with the Bank, provided that, in the event the Bank has given SP prior notice of a potential conflict, SP shall either obtain a waiver of both parties or in the absence of such waiver (which should not be unreasonably withheld or delayed), refrain from rendering similar services in a manner which would create a conflict with respect to such circumstances.

### **C. Management responsibilities**

Management of the Bank is responsible for establishing and maintaining the Bank's system of internal control. The Bank's management and the Audit Committee are responsible for the following:

- 1 Determining the scope, risk, and frequency of activities performed by SP
- 2 Evaluating the findings and results arising from the activities performed by SP
- 3 Evaluating the adequacy of the procedures performed by SP and the findings resulting from those activities, including actions by management, if any, necessary to respond to the findings and among other things, obtaining reports from SP
- 4 Ensuring that all information provided to SP is accurate and complete in all material respects contains no material omissions and is updated on a prompt and continuous basis. SP shall be entitled to rely on all information provided by and decisions and approvals of the Bank in connection with SP's work. SP will not be responsible if any information provided by the Bank is not complete, accurate or current. In addition, the Bank will also be responsible for obtaining all third-party consents and security clearances required to enable SP to access and use any third-party products necessary to our performance

#### **D. Relationship of Parties**

1. **Independent Contractor:** Nothing herein contained will be construed to imply a joint venture, partnership, Principal-agent relationship or co-employment or joint employment between the Bank and SP. SP, in furnishing services to the Bank hereunder, is acting only as an independent contractor. SP does not undertake by this Agreement or otherwise to perform any obligation of the Bank, whether regulatory or contractual, or to assume any responsibility for the Bank's business or operations. The parties agree that, to the fullest extent permitted by applicable law; SP has not, and is not, assuming any duty or obligation that the Bank may owe to its customers or any other person.
2. **Concerning Employees:** Personnel supplied by either party will be deemed employees of such party and will not for any purpose be considered employees or agents of the other party. Except as may otherwise be provided in this Agreement, each party shall be solely responsible for the supervision, daily direction, and control of its employees and payment of their salaries (including withholding of appropriate payroll taxes), workers' compensation, disability benefits, and the like.

#### **E. Testing Services**

1. If the Services include testing, penetration, intrusion or analysis of the Bank's information systems or enterprise whether by using intrusive or passive techniques and software tools ('Testing Services'), the provisions of this Section E shall apply and the Bank hereby consents to SP performing the Testing Services.
2. If the testing services involve third party SPs, the Bank shall obtain all necessary consents of third party SPs. This consent shall be in the form attached to this letter.
3. The Bank understands that Testing Services may result in disruptions of and/or damage to Client's or third party's information systems and the information and data contained therein, including but not limited to denial of access to a legitimate system user, automatic shutdown of information systems caused by intrusion detection software or hardware, or failure of the information system. The Bank is solely responsible for understanding the testing steps that will be performed as part of the Testing Services and for arranging alternative means of operation should such disruptions or failures occur and for all damage caused by the Testing Services. SP shall have no responsibility or liability for, and the Bank shall have no recourse against, SP or its partners, employees, agents or consultants for any damages as a result of such Testing Services.
4. The Bank shall have no recourse against, and shall bring no claim (in the nature of contribution or otherwise) against, SP, its subcontractors or their respective partners, officers, directors, agents, consultants and employees with respect to (i) any third-party claim (from all causes of action of any kind, including contract, tort or otherwise) against the Bank or its subsidiaries or affiliates related to or arising out of the Testing Services provided hereunder, or (ii) any losses, liabilities, damages or expenses (including attorneys' fees and expenses) incurred by the Bank or its subsidiaries or affiliates as a result of any such third-party claim. In addition, the Bank shall indemnify and hold harmless SP, its subcontractors and their respective partners, officers, directors, agents, consultants and employees ("SP Indemnitees") from and against (i) all claims and causes of action of any kind, including contract, tort or otherwise, by any third party related to or arising out of the Testing Services provided hereunder, and (ii) any losses, liabilities, damages and expenses (including, but not limited to, reasonable attorneys' fees and expenses incurred by the SP Indemnitees in any action or proceeding between an SP Indemnitee and any third party or

otherwise) that are incurred by the SP Indemnitees as a result of any such claims or causes of action. The Bank shall reimburse the SP Indemnitees for such Indemnified Costs as they are incurred by the SP Indemnitees. The Bank's subsidiaries and affiliates are deemed a third party as that term is used in this section E.

#### **F. Other Provisions**

1. Applicable Law; Severability: This Agreement shall be governed by the laws of the Union of India. If any portion of this Agreement is held to be void, invalid, or otherwise unenforceable, in whole or part, the remaining portions of this Agreement shall remain in effect.
2. Assignment: Neither this Agreement, nor any rights or obligations hereunder, may be assigned, in whole or in part, by either party without the prior written permission of the other party; provided that, upon written notice to the other, either party may assign this Agreement to a corporation or legal entity that acquires substantially all of or a controlling interest in that party ('Change of Control'), and SP may assign this Agreement to any member or affiliated firm of Ernst & Young Global Limited or Ernst & Young International, Ltd.
3. Entire Agreement; Applicable Law: This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof and supersedes all agreements and understandings between the Bank and SP with respect to the subject matter hereof made prior to the date of this Agreement. Each of the Bank and SP confirms that it has the right, power and authority to execute and deliver this Agreement and that it will be enforceable in accordance with its terms.
4. Term: The term of this Agreement shall commence on the date of the Engagement Letter ("Effective Date of contract") and shall continue up to the completion of the engagement ("Term") until terminated by either party through prior notice.
5. Transition After Termination: Upon the termination of this Agreement, SP shall, subject to the timely payment to it of all amounts owed hereunder, and the payment during the period of transition of its fees at its then-applicable hourly rate and its expenses, cooperate with the Bank in the orderly transition of its responsibilities to its successor, whether that be personnel employed by the Bank or an entity retained by the Bank for such purpose. In connection with such transition, SP will (a) continue to provide services contemplated hereunder for a reasonable period of time and, should the Bank desire, provide such services in coordination with the successor; and (b) make its personnel available at times mutually agreeable to discuss its work and transition issues with the Bank and the successor.
6. Non-Solicitation of Personnel: The Bank shall not solicit for employment or hire any SP employee who is involved in the performance of this Agreement during the term of this Agreement and for a period of twelve months following its termination except as may be agreed to in writing by both parties. In case the Bank does so, it will have to pay SP a sum equivalent to twelve months Cost to Bank of such employee.
7. Indemnity and Hold Harmless: The Bank shall indemnify and hold harmless EY and its personnel and subcontractors (collectively, the 'Indemnified Parties') from and against any loss, cost, damage and expense. (including but not limited to attorneys' fees) incurred by any Indemnified Party relating

to any claims arising out of or in any way relating to the Services or this agreement. This provision shall survive the termination of this agreement for any reason.

8. Changes and Delays: Changes in the type or extent of the services requested by the Bank or that are required for any other reason including any change in applicable law, professional standards or schedule delays or other events beyond a party's reasonable control (collectively, 'Unexpected Events'), may require fee and / or date of performance revisions to be agreed upon by both parties. If either party's performance is delayed or suspended as a result of Unexpected Events, and without its fault or negligence, then the period during which the services are to be performed shall be extended to the extent of such delay and neither party shall incur any liability to the other party as a result of such delay or suspension.
9. Conflict and survival: In the event if any conflict, ambiguity or inconsistency between this Annexure, the main engagement letter and any other document to which this Annexure 1 may be annexed or which may be annexed to this Annexure 1, including any terms and conditions on the Bank's purchase orders or otherwise, the terms and conditions of this Annexure 1 shall govern. The provisions of this Agreement that give the parties rights beyond termination of this Agreement will survive any termination of this Agreement.
10. Use of SP's name: Except as may be expressly permitted by this Agreement, the Bank shall not use or publicise SP's name, trademark, service mark or logo in connection with the Services, without the prior written consent of SP, which may be subject to certain conditions, in SP's discretion.
11. Internet e-mail: The Bank acknowledges that: (i) SP, the Bank and others participating in this engagement may correspond or convey documentation via Internet e-mail unless the Bank expressly requests otherwise, (ii) no party has control over the performance, reliability, availability, or security of Internet e-mail, and (iii) SP shall not be liable for any loss, damage, expense, harm or inconvenience resulting from the loss, delay, interception, corruption, or alteration of any Internet e-mail due to any reason beyond SP's reasonable control.

## **DISPUTE RESOLUTION PROCEDURES**

The following procedures shall be used to resolve any controversy or claim ('dispute') as provided in our engagement letter to which this annexed. If any of these provisions are determined to be invalid or unenforceable, the remaining provisions shall remain in effect and binding on the parties to the fullest extent permitted by law.

### ***Mediation***

A dispute shall be submitted to mediation by written notice to the other party or parties. The mediator shall be selected by agreement of the parties and any mediator so designated must be acceptable to all parties.

If the parties cannot agree on a mediator, a mediator shall be designated by the Indian Council of Arbitration ('ICA') at the request of a party. Any mediator so designated must be acceptable to all parties. The mediation shall be conducted as specified by the mediator and agreed upon by the parties. The parties agree to discuss their differences in good faith and to attempt, with facilitation by the

mediator, to reach an amicable resolution of the dispute. The mediation shall be treated as a settlement discussion and therefore shall be confidential. The mediator may not testify for either party in any later proceeding relating to the dispute. No recording or transcript shall be made of the mediation proceedings.

Each party shall bear its own costs in the mediation. The fees and expenses of the mediator shall be shared equally by the parties.

### ***Arbitration***

If a dispute has not been resolved within 90 days after the written notice beginning the mediation process (or a longer period, if the parties agree to extend the mediation), the mediation shall terminate and the dispute shall be settled by arbitration. The arbitration will be conducted in accordance with the procedures in this document and the Rules of the Indian Council of Arbitration ('Rules') as in effect on the date of the engagement letter, or such other rules and procedures as the parties may designate by mutual agreement. In the event of a conflict, the provisions of this document will control.

The arbitration will be conducted before a panel of three arbitrators appointed as per the Rules of the Indian Council of Arbitration ('Rules'). Any issue concerning the extent to which any dispute is subject to arbitration, or concerning the applicability, interpretation, or enforceability of these procedures, including any contention that all or part of these procedures are invalid or unenforceable, shall be governed by the currently applicable Indian Arbitration & Conciliation Act and resolved by the arbitrators. No potential arbitrator shall be appointed unless he or she has agreed in writing to abide and be bound by these procedures.

The arbitration body shall have no power to award non-monetary or equitable relief of any sort. It shall also have no power to award (a) damages inconsistent with any applicable agreement between the parties or (b) Punitive damages or any other damages not measured by the prevailing party's actual damages; and the parties expressly waive their right to obtain such damages in arbitration or in any other forum. In no event, even if any other portion of these provisions is held to be invalid or unenforceable, shall the arbitration panel have power to make an award or impose a remedy that could not be made or imposed by a court deciding the matter in the same jurisdiction.

Discovery shall be permitted in connection with the arbitration only to the extent, if any, expressly authorized by the arbitration panel upon a showing of substantial need by the party seeking discovery.

All aspects of the arbitration shall be treated as confidential. The parties and the arbitration panel may disclose the existence, content or results of the arbitration only as provided in the Indian Arbitration & Conciliation Act. Before making any such disclosure, a party shall give written notice to all other parties and shall afford such parties a reasonable opportunity to protect their interests.

The result of the arbitration will be binding on the parties, and judgment on the arbitration award may be entered in any court having jurisdiction in India.

ANNEXURE – A

SCOPE OF AUDIT

The details provided in the scope are indicative lists but not restricted to the following.

**(A) Audit of Information Security Architecture & Implementation of Information Security Policy with specific reference to:**

**Area:1** –

1. Information Security Organisation Structure
2. Roles and Responsibilities
3. Data Classification Policy
4. Software Policy
5. Application Security Policy
6. ATM Application Security
7. Electronic Payment System
8. Password Security Policy
9. Internet Banking Policy
10. Data Centre Security & Monitoring
11. Virus control Policy
12. Backup Policy
13. Data center policy
14. Network policy
15. Hardware policy
16. Physical security policy
17. Environment security policy
18. Incident Management Policy
19. Business continuity and Disaster recovery plan

**(B) IS Audit of key IT Systems and resources**

**Area:2 - Network Management & Security Audit:**

1. *Network admission control*
2. *Hardening of systems, switches and routers*
3. *Patch update Management*
4. *Port based security controls*
5. *Process control for change management*
6. *security incident and management*
7. *access control for DMZ application*
8. *control filtering for web access and data leakage*
9. *Net scanning-vulnerability assessment*
10. *Network admission control, hardening of system, switches routers, port based security control*
11. *Penetration testing (both internal and external)*
12. *Password cracking*
13. *Intrusion detection system testing*
14. *Router testing*
15. *Denial of Services testing*
16. *While doing the penetration test on server in live environment the ISA should ensure optimum performance of the System.*



17. *Audit of Network design from security, integrity and availability point of view.*
18. *Audit of setting of Network equipment from security and functionality point of view*
19. *Evaluation of Firewall policy and its implementation..*
20. *Network performance testing (including suggestions for increasing the performance)*
21. *Review of appropriateness of the network topology*
22. *Review of adequacy or otherwise of the hardware installed.*
23. *Network stress / Load test*
24. *Network Information Security and Administration (Public Key Infrastructure, Authentication, Access control, operating system controls etc.) of Key Applications Assessment (ATM, Internet Access, Anti-Virus, E-mail, ABB, RTGS, etc.)*
25. *The Bank's WEB-site and server*

**Area:3 – Data Centre - CBS Operations:**

**(1) IS Audit of Data Centre operations for Core Banking System-**

**(2) Physical security**

- a) *Physical access controls;*
- b) *Environment management systems such as electrical supply, UPS, air-conditioning, fire detection and suppression, generator, etc.*

**(3) Operating System (OS)**

- a) *Set up and maintenance of operating system parameters;*
- b) *Updating of OS Patches;*
- c) *OS Change Management Procedures;*
- d) *Use of root and other sensitive passwords;*
- e) *Use of sensitive system software utilities;*
- f) *Interfaces with external applications (such as other electronic channels in the case of CBS and other external ATM switches such as Cashtree in the case of the ATM system);*
- g) *Hardening of Operating System.*

**(2) Application software - Finacle (CBS and Other interfaces, if any )**

- a) *Authorisation Control such as concept of maker checker, exceptions, overriding exceptions, and error conditions.*
- b) *Authentication mechanism.*
- c) *User Management & Password Management*
- d) *Parameter Maintenance*
- e) *Access rights;*
- f) *Access logs/ Audit Trail generation;*
- g) *Change management procedures including procedures for testing;*
- h) *Documentation of change management;*
- i) *Documentation of Data Centre Operations.*

**(3) DBMS and data security**

- a) *Secure use of SQL;*
- b) *Control procedures for changes to the parameter files;*
- c) *Logical access controls;*

- d) Control procedures for sensitive database passwords;*
- e) Control procedures for purging of Data Files;*
- f) Procedures for data backup, restoration, recovery and readability of backed up data.*

**Area:4- Disaster Recovery Site - BCP:**

*IS Audit of DR Site with respect to*

1. Compliance with Bank's Disaster Recovery Plan aspects
2. Log shipping management

Review the Disaster Recovery Plan/Procedures documented for Core Banking Solution and its implementation by the prime vendor at the Data Centre and Disaster Recovery Centre

**Area:5– IT Products :**

**(A) ATM Centre and Card operations and Reconciliation:**

*IS Audit of ATM centre card operational processes with respect to*

- 1. PIN Management*
- 2. Card Management*
- 3. Delivery of ATM cards/ PINs to customers*
- 4. Hot listing of cards*
- 5. Customer dispute resolution*
- 6. Reconciliation within the Bank and with settlement agency/Banks*
- 7. ATM Network Security Architecture Analysis*
- 8. ATM functionality audit,*
- 9. ATM Switch,*
- 10. ATM Switch Reconciliation,*
- 11. Vulnerability analysis of ATM Network,*
- 12. Database controls,*
- 13. Backup & Recovery,*
- 14. Analysis of administrative procedures,*
- 15. Outsourcing arrangements,*
- 16. ATM sharing arrangements with other Banks/Visa and other agencies and compliance thereof.*

**(B) ABB Management and Reconciliation**

IS audit of ABB centre operational processes with respect to

1. Present system of ABB management
2. Control and security of interfaces of ABB
3. Adequacy of audit trails – Authentication mechanism, customer dispute resolution, reconciliation of ABB transactions

**(C) Internet/Mobile Banking:**

1. To Assess Flaws in Web hosting Software i.e Security of web server and e Design of the Applications.
2. Attempting to guess passwords using password-cracking tools.
3. Search for back door traps in the software.
4. Attempting to overload the systems using Distributed Denial of Services (DDOS) and Denial of Services (DOS) attacks.
5. Attempting penetration through perceivable network equipment/addressing and other vulnerabilities.
6. Check Vulnerabilities like IP Spoofing, Buffer Overflows, session hijacks, account spoofing, Frame Spoofing, Caching of web pages, Cross site scripting, Cookie handling, injection flaws
7. Check system of penetration testing and its effectiveness
8. Sniffing.
9. 128-bit SSL Certificate & PKI verification.
10. Whether solution architecture provides 24 X 7 availability to customer . If all servers are configured to synchronize time with Central NTP server.
11. To check whether date and time stamp are appearing correctly on all reports.
12. To check whether servers are updated with latest security patches. Remote server Management Software used, Web logic server is up to date, IOS version in Router is vulnerable one.
13. Confirm Rule base in Firewall are configured properly.
14. To ascertain IDS is configured for intrusion detection, suspicious activity on host are monitored and reported to server, firewall and IDS logs are generated and scrutinized. IP routing is disabled.
15. For changing system parameters whether Maker-Checker concept is followed.
16. Logical Access Controls Techniques viz. Passwords, Smart Cards or Other Biometric Technologies.
17. Proxy Server is issued between Internet and proxy systems.
18. Vulnerabilities of unnecessary utilities residing on Application server.
19. Computer Access, messages are logged and security violations reported and acted upon.
20. Effectiveness of Tools being used for monitoring systems and network against intrusions and attacks.
21. Proper infrastructure and schedule for back up is fixed, testing of back-up data done to ensure readability.
22. Legal issues.
23. Electronic Record is authenticated by Asymmetric Cryptosystem and hash function.
24. Secrecy and confidentiality of Customer preserved.
25. If any cases of unauthorized transfer through hacking, denial of service due to Technological failure is brought.
26. Regulatory and Supervisory issues.
27. Any other items relevant in the case of security.
28. All the guidelines issued by RBI and CERT-IN from time to time relating to Internet Banking Application and Bank's Official Website/Web hosting Software should be adhered to.

**ANNEXURE - B**

**Commercial Bid Format**

<b>Area No.</b>	<b>Major Audit areas</b>	<b>Audit fees ( A)</b>	<b>Taxes (B)</b>	<b>Total (A+B)</b>
1	IS Audit Implementation of Information Security Policy			
2	Network Management & Security Audit			
3	Data Centre - CBS Operations			
4	Disaster Recovery Centre – BCP			
5	IT Products			

**ANNEXURE - C**

**(On bidder's official letter head)  
Compliance Certificate**

To,

Date :

**The Asst. General Manager  
Inspection & Internal Audit Dept.  
Dena Bank H.O.  
4<sup>th</sup> Floor, Mumbai Main Branch  
17, Horniman Circle, Fort  
Mumbai – 400 001**

Dear Sir,

Ref: -

- 1) 1. Having examined the Tender Documents including all annexures, the receipt of which is hereby duly acknowledged, we, the undersigned offer to conduct the above audits.
- 2) 2. If our Bid is accepted, we undertake to complete the project within the scheduled time lines.
- 3) 3. We confirm that this offer is valid for six months from the last date for submission of Tender Documents to the Bank.
- 4) 4. This Bid, together with your written acceptance thereof and your notification of award, shall constitute a binding Contract between us.
- 5) 5. We undertake that in competing for and if the award is made to us, in executing the subject Contract, we will strictly observe the laws against fraud and corruption in force in India namely "Prevention of Corruption Act 1988".
- 6) 6. We agree that the Bank is not bound to accept the lowest or any Bid that the Bank may receive.
- 7) 7. **We have never been barred/black-listed by any regulatory / statutory authority.**
8. No legal case of any default / blacklisting should have ever been filed by any regulator on the firm.
- 8) **Enclose all annexures (1 to 9, D,E, F1,F2,G1,G2,G3,G4,G5)**

Signed Dated

Seal & Signature of the bidder

**ANNEXURE - D**

**Comments on the Terms & Conditions, Services and Facilities provided:**

Please provide your comments on the Terms & conditions in this section. You are requested to categorize your comments under appropriate headings such as those pertaining to the Scope of work, Approach, Work plan, Personnel schedule, Terms & Conditions etc. You are also requested to provide a reference of the page number, state the clarification point and the comment/ suggestion/ deviation that you propose as shown below.]

<b>Sr. No.</b>	<b>Page #</b>	<b>Section/ Point #</b>	<b>Clarification point as stated in the tender document</b>	<b>Comment/ Suggestion/ Deviation</b>
1				
2				

## **ANNEXURE - E**

### **Bidder's profile with the details of past experience:**

Sln.	Particulars	Details furnished by the bidder
1	Name of the bidder	
2	Year of establishment and constitution Certified copy of "Partnership Deed" or "Certificate of Incorporation" should be submitted as the case may be.	
3	Location of Registered office /Corporate office and address	
4	Mailing address of the bidder	
5	Names and designations of the persons authorized to make commitments to the Bank	
6	Telephone and fax numbers of contact persons	
7	E-mail addresses of contact persons	
8	Details of business and business background Service Profile & client profile	Enclose as Annexure – 1
9	Details of experience/knowledge possessed in the areas of Project Planning and management review, Resource Planning, Role and Responsibility definition, Co-ordination across multiple teams, Project risk analysis and containment	Enclose as Annexure – 2
10	Gross revenue of the bidder (not of the group) Year 2005-06 Year 2006-07 Year 2007-08	Total (for IS Auditing only)  CA certified financials – Enclose as Annexure – 3
11	Net Profit of the bidder (not of the group) Year 2005-06 Year 2006-07 Year 2007-08	CA certified financials – Enclose as Annexure – 4
12	Details of the similar assignments executed by the bidder in the (Name of the Bank, time taken for execution of the Assignment, total fees received and documentary proofs from are to be furnished)  The Auditee's completion certificate with the details of area, duration, fees paid and completed on. This is mandatory document to evaluate the pre-qualification Criteria and technical evaluation.	Enclose as Annexure – 5
13	Details of the similar assignments executed by the bidder in other than Banking industry (Name of the Organisation, time taken for execution of the assignment, total fees received and documentary proofs are to be furnished)  The Auditee's completion certificate with the details of area, duration, fees paid and completed on.	Enclose as Annexure – 6

	This is mandatory document to evaluate the pre-qualification Criteria and technical evaluation.	
14	Names of team members identified for this assignment and their professional qualifications and experience/expertise Details of similar assignments handled by the said team members Documentary proofs for all the assertions are to be enclosed	<b>As per annexure F1</b>
15	Details of other professional in the organization	<b>As per annexure F2</b>
16	Details of lead audit certification from leading certification bodies	Enclose as Annexure – 7
17	Effort estimate and elapsed time are to be furnished in annexure G - Area wise	<b>As per annexure G1,G2,G3, G4,G5</b>
18	Details of inputs, infrastructure requirements required by the bidder to execute this assignment - Area wise	Enclose as Annexure – 8
	Details of the bidder's proposed methodology/approach for providing services to the Bank with specific reference to the scope of work - Area wise.	Enclose as Annexure – 9
	Details of deliverables the bidder proposes with specific reference to the scope of work - Area wise.	Enclose as Annexure – 10

**Declaration :**

1. We confirm that we will abide by all the terms and conditions contained in the RFP.
2. We hereby unconditionally accept that Bank can at its absolute discretion apply whatever criteria it deems appropriate, not just limiting to those criteria set out in the RFP, in short listing of bidders.
3. All the details mentioned by us are true and correct and if Bank observes any misrepresentation of facts on any matter at any stage, Bank has the absolute right to reject the proposal and disqualify us from the selection process.
4. We confirm that this response, for the purpose of short-listing, is valid for a period of six months, from the date of expiry of the last date for submission of response to RFP.
5. We confirm that we have noted the contents of the RFP and have ensured that there is no deviation in filing our response to the RFP and that the Bank will have the right to disqualify us in case of any such deviations.

Place :

Date :

Seal & Signature of the bidder



**ANNEXURE – F**

**Proposed Team Profile**

Documentary proofs are to be enclosed to substantiate the claims made.

<b>Mem ber no. M1 M2 Etc.</b>	<b>Name of Proposed Auditor</b>	<b>Prof. Qualificat- ions</b>	<b>Certifications/ Accreditations</b>	<b>Banking Solutions expertise (Mention if he has worked in Banks earlier) In terms of years and areas of expertise</b>	<b>IT Expertise In terms of years and areas of expertise</b>	<b>Number of similar assignments involved In Banks in India</b>

**ANNEXURE – F1 Proposed Team Profile**

**ANNEXURE – F2 Other staff in the SP**

**ANNEXURE – G**

**Estimated Effort and Elapsed Time for each audit area (Annexure – G1 for ISP, Annexure – G2 for NMS, etc.)**

<b>Sl No</b>	<b>Activities for Area-1/2/3/4/5</b>	<b>Elapsed time</b>	<b>Effort in Man days</b>	<b>Member who will be deployed (M1/2..)</b>	<b>Annexure-A Ref.no.</b>	<b>Tools used</b>	<b>Deliverables</b>
--------------	--------------------------------------	---------------------	---------------------------	---	---------------------------	-------------------	---------------------

The above audit shall be completed with a total \_\_\_\_\_ man days.

The above activities can be started from \_\_\_\_\_ to \_\_\_\_\_  
if the Bank issues LoA on 28-11-08.

**ANNEXURE – G1**

**ANNEXURE – G2**

**ANNEXURE – G3**

**ANNEXURE – G4**

**ANNEXURE – G5**

Place:

Date:

Seal and Signature of Bidder:

**End of Document**