Continuous Information System Audit

of

Data Centre & Project Office

2013

Tender Ref: HO/INSP/3960/2013 dtd. 27-02-2013
Request for Proposal (RFP) issued by
Deputy General Manager (Inspection)

Section ï I

1. Introduction and Disclaimer

This Request for Proposal document (ñ**RFP**ò) has been prepared solely to enable Dena Bank ñ**Bank**ò) in the selection of suitable organization (Service Provider ï 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 (ñthe **Recipien**tòor ñthe **Responden**tò) and no other person or organization.

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 organizations, 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

One (1) Hard copy duly signed by authorized person and one (1) electronic copy (excluding commercial bid) in MS-Word format on CD ROM should to be submitted to ñBankôs Evaluation Officeòat the following address:

The Deputy General Manager
Dena Bank H.O.
Inspection & Internal Audit Dept.
4th Floor, 17-Horniman Circle
Fort, Mumbai – 400001.

12.1 Submission will be valid if:

- Application Money is paid before pre-bid meeting by those attending the pre-bid meeting.
- Copies of the RFP are submitted before the scheduled closing time.
- Bids are submitted in two separate sealed envelopes with separate marking ñTechnical Proposalò& ñCommercial Proposalò
- All separate copies of RFP and attachments must be provided in a sealed envelope or sachet ñ
- Soft copies of all Annexures must be provided on a CD
- EMD is enclosed only in the ñTechnical Proposalò

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). 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 the 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. Tender Validity Period

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

12.4. Requests for Information

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

Mr Raj Shekhar
Information System Audit Head
Dena Bank H.O.
4th Floor, 17-Horniman Circle
Fort, Mumbai – 400001.
Mobile : 9617206944

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 Respondent after the tender closes and all such information and material provided must be taken to form part of that Respondentôs 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 Respondentõs 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 an 8 stages approach.

1. Issue of Tender Notification:

This RFP is made available at the Bankõs web site www.denabank.com under tenders. And also send by e-mail/post to the current CERT-In empanelled organizations as per list available on website of CERT-IN.

2. Pre-bid meeting:

The pre-bid meeting will be organized at - **Dena Bank, Dena Corporate Centre, C-10, G Block, Bandra Kurla Complex, Bandra (East), Mumbai – 400051)** 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 attended the meeting 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. Sale of RFP

4. Submission of RFP

15.1. Checklist for Continuous IS Audit.

The SP has to submit their proposed checklist for audit of Critical issues on Concurrent basis including the following.

1.	Change in Daily Bulk & Flexi Interest Rates
2.	Incorporation of Revised Interest Rate changes of Deposit and Advances as per H.O., guidelines.
3.	User Management
4.	Addition / Modification in GSPM (General Scheme Parameter Maintence) ï Due to changes
5.	Parameter level changes made in MOPM (Menu Option Maintenance.
6.	Parameter level changes made in EXCDM (Exception Code Maintenance).
7.	Parameter level changes made in ACMDB (Office Account Maintenance).
8.	Creation of New GL, sub GL, Currency, Office account in Finacle.
9.	TDS parameters
10.	Change Management Requests - vetting documents before moving any customization to Production sever & DR server
11.	Incorporation of revised Service Charges as per H.O., Guidelines.
12.	Daily Batch Jobs which have failed and intimated by Wipro technical team.
13.	Deployment of patches if any received from Infosys in Production Server & DR server
14.	Abnormal / Exceptional Transactions in CBS
15.	Global processes such as interest application, recovery of charges, etc.
16.	CBS Database - Oracle back-end updates
17.	ADS Server ï DBA activities
18.	Internet / Mobile Server ï DBA activities
19.	Review of Helpdesk Calls to identify root cause of problems
20.	IS Security Policy Bankôs or other guidelines implementation
21.	Sol creation
22.	SCFM parameters
23.	Consistency of Application & Databases (DC, DR & NDR)
24.	Reversal of proxy transactions

The SP should submit the Audit Checklist covering the above as Annexure ï A1. If they want to add any other points, it should be separately numbered from 101.

5. Evaluation of RFP

6. Presentation

The qualified SP should given their presentation covering the above day to day audit checklist, their audit approach / methodology to cover entire scope and its timely reporting as per Bankôs schedules.

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

15.2. 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.

Description	Due Dates
Commencement of sale of RFP	01.03.2013
Closure of sale of RFP	07.03.2013
Pre ï bid meeting	09.03.2013 at 10.30 am
Submission of RFP	18.03.2013 before 2:30 pm
Opening of RFP	18.03.2013 at 3pm
Presentation by the SP	19.03.2013
Evaluation & Issuance of LoA	25.03.2013
Acceptance of LoA	28.03.2013
Commencement of Continuous IS Audit	01.04.2013

* 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 **Shri. 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. Under the provisions of the Banking Regulations Act 1949, in addition to the business of banking, the Bank can undertake other business as specified in Section 6 of the Banking Regulations Act, 1949.

The present organisational structure of the Bank consists of four tiers viz., Corporate Office (CO), General Manager Offices (GMO), Regional Offices (RO) and Branches. CO, consisting of various functional departments deals with mainly policy formulation, setting of targets and monitoring of performance. The Bank has set up 4 GMOs and 21 Regional Offices to exercise immediate supervision and control over the branches under their jurisdiction. The Bank has a network of 1368 branches spread across the length and breadth of the country

.

The Bank also has specialized branches catering to the specific needs of Retail customers, Industrial units, corporate clients, Forex dealers, Exporters and Importers, Small Scale Industries and Agricultural sector. The Bank has sponsorship in 2 Regional Rural Banks (RRB).

Bank has implemented Core Banking Solution - Finacle from Infosys. Presently all the 1368 branches and ROs are connected to the CBS. The Data Center of the Bank and the CBS Project Office of the Bank are located at Jogeshwari-West, Mumbai

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 D/R Data Centre is located at Bangalore.

Bank's Mission

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

<u>CBS and Other Details</u>

First branch was migrated to CBS on 12th March 2007. All branches have been brought under the CBS platform covering **737 centers / 21 Regions (Excluding HO) / 28 States & Union Territories**.

Bank has set up its own network named as ñDENANETò using 1647 Leased Lines, **788** ISDN PRI/BRI lines and 303 VSATs connecting all branches, **30** administrative offices spread over 300 centers. This network supports Bankôs inter ï connected ATMs seamlessly. Critical applications like Internet / Mobile Banking and NEFT / 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.

Data Centre & Project Office : ***Jogeshwari (W), Mumbai***
DR Site : ***Electronic City, Bangalore***
Near DR Site : ***Vikhroli, Mumbai***

Location	***: No. of Servers***	***Firewalls***	***Routers***	***Switches***	***NIPS***
Data Centre & HO-BKC:	***123+36***	***6+4***	***14+6***	***14+2***	***4+0***
DR Site :	***44***	***6***	***12***	***12***	***6***
Near DR :	***10***	***2***	***4***	***8***	***0***

A total of 531 ATMs have been installed all over the country. Out of these ATMs, 424 are On site and 107 are Off site . With a view to expand the ATM access to our customers for carrying banking transactions, we have also tied up with the following banks and ATM networks for mutual sharing of ATMs:

1. Cash tree group of Banks

   (Bank of India, United Bank of India, Syndicate Bank, Indian Bank, Union Bank of India, Bank of Rajasthan, Indian Overseas Bank, Karnataka bank, Yes Bank, Dhanalakshmi Bank Ltd etc)

3. Cash net group of Banks
   (Axis Bank, Citibank, Corporation Bank, Development Credit Bank, Deutsche Bank, HDFC, IDBI Bank, HSBC, Standard Chartered Bank, ING Vysya Bank, Barclays, Kotak Mahindra Bank and Dhanalakshmi Bank Ltd)

4. National Financial Switch (NFS) group of Banks
   (Allahabad Bank, Andhra Bank, Axis Bank, Bank of Baroda, Bank of India, Bank of Maharashtra, Canara Bank, Corporation Bank, Central Bank of India, HDFC Bank, ICICI bank, IDBI, Indian Bank, Indian Overseas Bank, Punjab National Bank, State Bank of India, Syndicate Bank, UCO Bank, United Bank of India, Union Bank of India, Vijaya Bank etc)

5. VISA enabled ATM network

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

1. Assessing the security, availability and efficiency of IT assets of the Bank.
2. Assessing the confidentiality, integrity and availability of information system
3. Assessing the integrity of general operating system, Database, Network connectivity, Network equipment, Telecommunication equipment, any special security infrastructure such as biometric equipment.
4. Assessing the integrity of sensitive and critical application systems environment, including financial and management information.
5. Assessing the efficiency and effectiveness of Information System.
6. The IS auditors will require to concentrate on the following to ensure that the Information Systems Assets of the organization are safeguarded:
   a) Environmental Security
   b) Data
   c) Uninterrupted Power Supply
   d) Electrical Lines
   e) Data Cables & Networking Products
   f) Fire Protection
   g) Insurance of Assets
   h) Annual Maintenance Contract
   i) Logical Security & Access Control - Operating System Level
   j) Logical Security & Access Control ï Application System Level
   k) Logical Security & Access Control ï Network System Level

7. Assessment of Fraud (risk of fraud ï internal and extrenal)
8. Gap Assessment for complying with RBI guidelines (Gopalakrishnan Committee)

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

2.2. Audit Approaches

Information Systems Audit will be facilitated through a combination of techniques and tools

Audit project planning
Documentation review
Manual and automated controls testing using IS audit checklists based on globally accepted standards and RBI guidelines/ Circulars / IT Act.

Audit reports:

- High level summary for the management
- Detailed findings along with recommendations
- Audit findings to be classified as Low, Medium, High within each specific audits

2.3 Audit Methodology

The IS audit work to include manual procedures, computer assisted procedures and fully automated procedures applicable. An audit project team, plan and audit schedule to be presented, discussed, approved and implemented.

2.4 Auditors:

Audit should be carried out by CERT-In empanelled audit firm by persons having **CISA/ CISSP / CISM / DISA** qualifications with at least two IS auditsôexperience.

The Core Audit Team proposed by the SP should be employers on the rolls of the SP. No part of the engagement shall be outsourced by the selected SP to third party vendor. SP must warrant that these key auditors to be displayed in this audit have been sufficiently involved in similar audits in the past. SP should ensure that the audit team is actively involved in the conduct of the audit. The audit of DCA should be carried out by team-A on daily visit to Data Centre and Project Office throughout the period of contract. Audit of other areas are to be carried out by team-B depends on the frequency of reporting with prior permission from the Bankôs IS Audit Head. The leader of the team-A shall be the single contact point or co-ordinator for all the activities mentioned in the RFP.

2.5 Audit Scope:

A description of the envisaged scope is enumerated in brief as under and an indicate detail in Section - V. 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 12 Areas as under:

Slno	Area	Details of area for audit
1	DCA	Data Centre & Project Office ï Continuous IS Audit (daily)
2	VAPT	VAPT
3	DRS	DRS site ï Bangalore
4	NDR	NDR ï Mumbai
5	SRP	Short Range IT Plans
6	NET	Network Management
7	ATM	ATM, Internet Banking / Mobile Banking / IT Products
8	PSW	Acquisition and Implementation of Packaged Software
9	ISW	Development of Software in-house and outsourced
10	OUT	Audit of Outsourcing Arrangements (all IT related services)
11	ISS	IS Security Policy (Implementation is verified in the above areas)
12	ISA	IS Audit Guidelines & Checklist

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 SPôs 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.

VAPT: The SP should carry out Vulnerability Assessment and penetration testing covering the operating systems, databases, network and security infrastructure and various on-line channels facing customers.

The SP shall review compliance done by Bank on the Audit observations of the Previous Audits of all areas. If Bank desires, then, during the review of compliance SP may be required to involve one representative of the IS Audit Cell to validate the checklist and guidelines provided by the SP.

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 ï the SP will deliver detailed reports (an indicative to cover area wise) as below:

- Verification and submission of compliance to previous audit as per the Bankôs format
- IS Audit (Technical & Process) Report of all the areas covering the objectives, efficiency and effectiveness
- Presentation to the Top Management of the findings of the Reports (quarterly)
- Risk Matrix Analysis Report
- Recommendations for Risk Mitigation
- Gap assessment and recommendation for mitigation
- Provide check list with guidelines for the subsequent audit (hard & soft copies)
- Provide re-designed network & security architecture along with technical specifications of network & security solutions (if any suggested during the review of IT infrastructure) based on the operational and business requirements of Dena Bank. These technical specifications can be used by Dena Bank for selecting products / solutions.
- The report findings should cover all the areas separately mentioned in the scope.
- The report findings should be submitted in PDF and MS Word formats.
- Day to Day observations (area- DCA) should be submitted in Excel format or on-line system available in the Bank
- Significant findings should be promptly communicated to the appropriate person prior to the submission of final report.
- All observations should be thoroughly discussed with process owner before finalization of report.

The Report should comprise of the following sub-reports:

Executive Summary: - An executive summary should form a part of the REPORT.

Core Findings along with Risk Analysis:

The SP will submit a report bringing out the core findings of the IS Audit exercise in the existing practices along with Risk Analysis of individual items , with reference to the best practices & standards.

2.6.1. Detailed Findings / Overall Risk rating:

The detailed findings of the Audit would be brought out in this report which will cover in details all aspects viz. identification of flaws / gaps /vulnerabilities in the systems (specific to equipments/resources ï indicating name and IP address of the equipment with Office and Department name) , identifications of threat sources , identification of Risk , Identification of inherent weaknesses ,Servers/Resources affected with IP Addresses etc. Report should classify the observations into Critical /Non Critical category and asses the category of Risk Implication as EXTREMELY HIGH/VERY HIGH/HIGH/MEDIUM/LOW RISK based on the impact. The Reports should be substantiated with the help of snap shots/evidences /documents etc. from where the observations were made. Suitable weightage to each observation must be given and the SP should arrive at the overall Risk rating, in terms of Scores.

In Depth Analysis of findings /Corrective Measures & Suggestions along with Risk Analysis

The findings of the entire IS Audit Process should be critically analyzed and controls should be suggested as corrective /preventive measures for strengthening / safeguarding the IT assets of the Bank against existing and future threats in the short /long term . Report should contain suggestions/recommendations for improvement in the systems wherever required. Also, if the formal procedures are not in place for any activity, evaluate the process & the associated risks and give recommendations for improvement as per the best practices.

2.6.2. Regulator compliance certificate:

During the audit regulatory compliance certificate should be provided by the SP and some indicative list is as under:

I) A certificate as per RBI guidelines of the Payment System Operated under the PSS Act,2007 (RBI circular No. DPSS.AD.No./ 1206/02.27.005/2009-2010 dated 7th December, 2009)

II) A certificate as per RBI guidelines for Internet Banking and Mobile Banking

III) IS Audit of RA Office certificate (IDRBT)

2.6.3. Reporting schedule:

Area	Details of area for audit	Reporting
DCA	Data Centre & Project Office ï Continuous IS Audit (daily)	Every Friday submission (soft copy) & consolidated Monthly by 10th of subsequent month
VAPT	VAPT	Quarterly by 10th of July, October, January & April Including compliance verification of all areas.Presentation to Management (Auditeeôs compliance ï Auditoròs performance review) and if any revisions proposed in the Checklist or any deliverable formats should be incorporated by the SP
DRS	DRS site ï Bangalore	
NDR	NDR ï Mumbai	
SRP	Short Range IT Plans	
NET	Network Management	Half yearly by 10th of October and April. Report-H1 to cover audit period April to September and H2 for October to March.
ATM	ATM, Internet Banking / Mobile Banking / IT Products	
PSW	Acquisition and Implementation of Packaged Software	
ISW	Development of Software in-house and outsourced	
OAI	Audit of Outsourcing Arrangements (all IT related services)	Yearly by 10th of April with coverage of period April to March and including compliance verification of all areas.
ISS	IS Security Policy	
ISA	IS Audit Guidelines & Checklist	

2.7. Duration of Audit:

The entire audit should be covered for the audit period is from 01-04-2013 to 31-03-2014 and the Bank may repeat the second audit period from 01-04-2014 to 31-03-2015 with the same SP. The Bank reserves the right to terminate the assignment, if the assignment is not proceeding in accordance with the terms of contract or to the satisfaction of the Bank by giving a notice of seven days. The Bank is not be liable for any fees or compensation incase the contract is terminated as above.

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 of Rs. 50 lacs each for the last two years.
2.8.3 The SP should be a profit making entity in the last 2 years
2.8.4 The SP should be empanelled by CERT-In (Indian Computer Emergency Response Team) for the period valid up to 31.03.2015
2.8.5 The SP should have a pool of resources (minimum 5 professionals) who possess certifications such as: CISA/ CISSP/ CISM / DISA
2.8.6 The SP should have conducted at least one audit of DC in any Scheduled Commercial Banks having not less than 500 branches in India.
2.8.7 Existing Dena Bankôs CBS consultant/supplier is not eligible to participate in the audit.
2.8.8 The SP should be a legal entity in India and have its registered Office in India.
2.8.9 The SP should not have been black ï listed by any Public Sector, RBI or IBA or any other regulator / statutory body.
2.8.10 The SP should not have audited area/ areas during the two previous audits of our Bank.

2.9. Earnest Money Deposit

Subject to compliance of Response Submission Process as elucidated in Section ï I, the intending bidders should pay along with bids an Earnest Money Deposit amount of Rs. 1,00,000/- (Rupees One Lac only).The EMD shall be paid by Demand Draft / Bankerôs Cheque / Pay Order drawn in favor of ôDena Bank ï A/c Inspection Departmentôpayable 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 ñLetter of appointmentòissued 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 15% of the first year total contract value. The validity of the guarantee would be 15 months from the date acceptance of first LoA.

- The unsuccessful bidders, only after acceptance of the ñLetter of Appointmentòby 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 / Bankerôs Cheque / Pay Order drawn in favor of ñDena Bank ï A/c Inspection Departmentôpayable at Mumbai. The application money is non-refundable. Application money is to be submitted on or before Pre-bid meeting .

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 CONTINUOUS IS AUDIT: TENDER REFERENCE NO. xxx.** on top of the envelope containing the technical bid and **"COMMERCIAL PROPOSAL FOR CONTINUOUS 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 CONTINUOUS 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.

The Commercial Proposal shall be submitted as per **Annexure - B.**

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

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 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:

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 Bankôs 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 ï 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 ñAgreed Professional Feeò. The SP should quote the fees for the second year also, because, in case the Bank desires the audit may be repeated with the same SP for the second year.

9. The bidder cannot change the DCA auditors during the audit 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 SPôs fees will be paid in the following manner for each item which is described in the Commercial bid (Annexure - B):

On completion audit, submission of audit findings, reports and other deliverables as per point No 2.5 & 2.6.

13. LIQUIDATED DAMAGES (LD) :

The Bank will impose liquidated damages, of amount quoted by the SP as per Annexure ï B (FD1 /SD1) per day for delay in not adhering to the time schedules (2.5 & 2.6) or auditorôs absent day.

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 Bankôs 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 that Bank may sustain on account of violation of patent, trademarks etc. by the bidder by executing an instrument to the effect on a Non-Judicial stamp paper.

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 SP or a Power of Attorney holder 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 contract price (FD1 /SD1).

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 also mentioned in RFP 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 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:

Parameter	Max. Marks	Proof for
No. of audits of DC, 8 marks for each different Bank	16	Audit conducted since 2010
No. of audits of CBS Finacle, 5 marks for each different Bank	10	Audit conducted since 2010
No of professionals with qualifications such as CISA/CISSP/CISM/DISA in SPôs muster roll. 1 mark for 1 employee	9	Staff as of 31-12-12
No of auditors with qualifications such as CISA/CISSP/CISM/DISA and audit experience in CBS ï Finacle (team deployed for DCA of our Bank: 10 mark for 1 such auditor)	20	Valid certificates of the identified auditor for the Bank
Presentation of Audit Checklist, audit approach, methodology reporting etc.	15	Presentation in Mumbai
Total Mark	70	

At the sole discretion 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 ï off **(TM-CO**) for opening of the commercial bid would be 50% . SPs scoring below the same would not be considered for commercial bid opening.

Bank may, at its sole discretion, decides 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.

All the proposals will be compared technically and commercially. Bank will give 70% marks to technical evaluation and 30% to commercial evaluation. The bidder scoring highest marks in technical Evaluation will be given 70 marks. The other biddersômarks score will be as follows.

Technical Evaluation Marks = ((Marks of bidder in Technical Evaluation) / (Total Marks of the Highest scoring Bidder in Technical Evaluation)) *70

Commercial Evaluation

Commercial Offer of only those SPs will be opened who have scored minimum 50% marks in technical evaluation. The bidder quoting lowest price will be given 30 marks. The other bidders will get marks as follows.

Commercial Evaluation Marks = (Cost quoted by lowest bidder) / (Cost quoted by the bidder) * 30)
Total marks in the Bid (TMB) = Technical Evaluation Marks + Commercial Evaluation Marks
The bidder scoring the highest total mark for the bid (TMB) will be declared L1 bidder

The contract will be awarded to the L1 bidder selected on the basis of the above criteria and he will be declared the successful bidder.

Empanelment:

The current audit assignment will be awarded to the L1 bidder, other qualified bidders will be ranked as per Total marks in the Bid (TMB) and placed in the empanelled list for the next 2 years period. In case of repeating for second audit period or cancellation of contract to L1 bidder or withdrawal / refusal by L1 bidder, the empanelled bidders may be assigned the same audit as per descending TMB for the period of 12 months or remaining period out of 24 months whichever is less.

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 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 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 to 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 at 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.

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 Bankôs system of internal control. The Bankôs management and the Audit Committee are responsible for the following:

- Determining the scope, risk, and frequency of activities performed by SP
- Evaluating the findings and results arising from the activities performed by SP
- 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
- 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 SPôs 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 providing services to the Bank under the contract, 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 Bankôs 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), workersôcompensation, disability benefits, and the like.

E. 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 (a Change of Control), and SP may assign this Agreement to any member or affiliated firm of SP..

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 (ñEffective Date of contractò) and shall continue up to the completion of the engagement (ñTermò) 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. 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 partyôs reasonable control (collectively, ñUnexpected Eventsò), may require fee and / or date of performance revisions to be agreed upon by both parties. If either partyôs 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.

8. 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 Bankôs 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.

9. 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.

10. 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 partyÕs 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.

Section - V

SCOPE OF AUDIT

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

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) content filtering for web access and data leakage
9) Net scanning-vulnerability assessment
10) Penetration testing (both internal and external)
11) Penetration testing of internet facing servers (external)
12) Vulnerability Assessment (VA) of Servers, network devices and infrastructure components to identify vulnerabilities.

a. Identify and prioritize the risks
b. Provide recommendations for remediation

13) Password cracking
14) Intrusion detection system testing
15) Router testing
16) Denial of Services testing
17) While doing the penetration test on server in live environment the ISA should ensure optimum performance of the System.
18) Network design review from security, integrity and availability point of view.
    a. Review the appropriate segregation of network into various trusted zones
    b. Review the traffic flow in the network
    c. Review the existing routing policy
    d. Review the route path and table audit
    e. Review of routing protocols and security controls therein
    f. Review the security measures at the entry and exit points of the network
    g. Obtaining information about the architecture and address scheme of the network
    h. Checking Routing and Inter-Vlan Routing and Optimization.
    i. Checking of HSRP Configurations if any, and its working.
    j. Checking redundancy and Load Balancing as per the requirement.
    k. Routing Protocol Analysis
    l. Analyze protocols used and traffic generated and means to optimize traffic
    m. Analysis of load balancing mechanism
    n. Analysis of latency in traffic across various links

19) Audit of setting of Network equipment from integrity, security availability and functionality point of view
20) Evaluation of Firewall policy and its implementation..
21) Network performance testing (including suggestions for increasing the performance)
22) Network performance testing using automated tools (including suggestions for increasing the performance)
23) Analysis at link level
24) Analysis at application level
25) Review of appropriateness of the network topology

26) Review of adequacy or otherwise of the hardware installed.
27) Network stress / Load test
28) Audit Security Implementation of the Network based applications - ATM, Internet Access, Anti-Virus, E-mail, RTGS, etc.)
29) The Bankôs WEB-sites and server
30) Violation logging management
31) Implementation of Information Security Policy with reference to this Area
32) Implementation of IPv6 Policy as per circular issued by Ministry of Finance, Dep of Financial Services (P&C section) dated 12.08.2011
33) Gap assessment for complying with RBI guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds (Gopalakrishnan Committee recommendations. RBI circular no. RBI/2010-11/494 DBS.CO.ITC.BC.No: 6/31.02.008/2010-11 dated 29.04.2011) with specific reference to Information Security, Business Continuity Planning.

Disaster Recovery Site - BCP:

IS Audit of DR Site with respect to

1) Compliance with Bankôs Disaster Recovery plan aspects
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) Review & audit of drill activity between Primary site and disaster recovery site
4) Log shipping management, audit of Storage level synchronous/asynchronous replication between DC & DR Site.

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

Near DR - BCP:

IS Audit of NDR Site with respect to

1) Compliance with Bankôs Disaster Recovery plan aspects
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) Review & audit of drill activity between Primary site and Near DR Site (**for some future applications, Near DR Site will work as DR Site).**
4) Log shipping management, audit of Storage level synchronous/asynchronous replication between DC & NDR.

Data Centre - CBS Operations:

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

(i) Physical security

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

(ii) 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.

(iii) Implementation of Information Security Policy with reference to this Area

(iv) Gap assessment for complying with RBI guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds (Gopalakrishnan Committee recommendations. RBI circular no. RBI/2010-11/494 DBS.CO.ITC.BC.No: 6/31.02.008/2010-11 dated 29.04.2011) with specific reference to IT Operations, Information Security.

(v) Assessment of RCAs submitted by resp. vendors for the critical incidents occurred in Data Centre or DR or NDR Site.

(2) Application Review of Core Banking software - Finacle *(CBS) and Other applications viz., Treasury(KASTLE), RTGS, ALM (OFSA), AML(AMLOC), IRM (SAS),etc) and interfaces thereof.*

a. *Authorization 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.*
j. Study & review the implemented functionality of Finacle core banking solution & other applications in all the areas and to ensure correctness of functionality of each module and all modules in totality vis a vis availability of the functionality / features in the version currently implemented in the Bank.
k. Study the CBS& other applications for adequate input, processing and output controls and conduct various tests to verify existence and effectiveness of the controls .
l. Perform a test of controls and functionality setup in the Core Banking & other applications and to ensure that all the functionalities and controls are implemented properly and completely.
m. Review/audit the presence of adequate security features in CBS & other applications to meet the standards of confidentiality, reliability and integrity required for the application supporting business processes.
n. Identify ineffectiveness of the intended controls in the software and analyze the cause for its ineffectiveness. Review adequacy and completeness of controls
o. Review effectiveness and efficiency of the Applications.
p. Review of all controls including boundary controls, input controls, communication controls, database controls, output controls, interfaces controls from security perspectives.
q. Review of all Interface of application with other system OR interface of other system with applications for Security, accuracy, consistency and safety.

r. Identifying critical risk areas, control weakness in application systems and recommended corrective actions from security prospective.

(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.

(4) Audit of various payment and settlement systems operated under the PSS Act, 2007 implemented by Bank such as – SFMS, RTGS, NEFT, RD-NDS, CFMS, CCIL/Clearcorp applications such as CBLO, FX-CLEAR, FX-SWAP, NDS-OM, NDS-CALL and NDS – AUCTION as per terms of RBI circular No – DPSS.AD.No./1206/02.27.005/2009-10 dated 07.12.2009 (The SP is required to give a separate report for this audit)

Audit of Information Security Architecture & Review of Information Security Policy with specific reference to:

1) Information Security Organization 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
20) Internet Usage Policy
21) E-Mail Usage Policy
22) IS Audit Policy

Gap assessment for complying with RBI guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds (Gopalakrishnan Committee recommendations. RBI circular no. RBI/2010-11/494 DBS.CO.ITC.BC.No: 6/31.02.008/2010-11 dated 29.04.2011) with specific reference to Information Technology Governance, IS Audit, Customer Education, Legal Issues.

Out Sourcing Arrangement Review - All IT related services:

- The audit of the outsourced arrangements will be as per terms of RBI Circular No RBI/2006/167 DBOD.NO.BP.40/21.04.158/2006-07 dated 03.11.2006. The Audit will cover evaluation of the **financial and operational conditions** of the Service Provider, breach in security / confidentiality, non ï compliance with legal and regulatory requirement, Bank exposed to different types of risks which can lead to financial losses, loss of reputation to the Bank or systemic risk in wake of outsourcing.
- Gap assessment for complying with RBI guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds (Gopalakrishnan Committee recommendations. RBI circular no. RBI/2010-11/494 DBS.CO.ITC.BC.No: 6/31.02.008/2010-11 dated 29.04.2011) with specific reference to IT Services outsourcing

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.*
17) Implementation of Information Security Policy with reference to this Area

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,
7) Frame Spoofing, Caching of web pages, Cross site scripting, Cookie handling, injection flaws
8) Check system of penetration testing and its effectiveness
9) Sniffing.
10) 128-bit SSL Certificate & PKI verification.
11) Whether solution architecture provides 24 X 7 availability to customer . If all servers are configured to synchronize time with Central NTP server.
12) To check whether date and time stamp are appearing correctly on all reports.

13) To check whether servers are updated with latest security patches. Remote server
14) Management Software used, Web logic server is up to date, IOS version in Router is vulnerable one.
15) Confirm Rule base in Firewall are configured properly.
16) To ascertain IDS is configured for intrusion detection, suspicious activity on host are monitored and reported to server, firewall and IPS/IDS logs are generated and scrutinized. IP routing is disabled.
17) For changing system parameters whether Maker-Checker concept is followed.
18) Logical Access Controls Techniques viz. Passwords, Smart Cards or Other Biometric Technologies.
19) Proxy Server is issued between Internet and proxy systems.
20) Vulnerabilities of unnecessary utilities residing on Application server.
21) Computer Access, messages are logged and security violations reported and acted upon.
22) Effectiveness of Tools being used for monitoring systems and network against intrusions and attacks.
23) Proper infrastructure and schedule for back up is fixed, testing of back-up data done to ensure readability.
24) Legal issues.
25) Electronic Record is authenticated by Asymmetric Cryptosystem and hash function.
26) Secrecy and confidentiality of Customer preserved.
27) If any cases of unauthorized transfer through hacking, denial of service due to Technological failure is brought.
28) Regulatory and Supervisory issues.
29) Any other items relevant in the case of security.
30) 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.
31) Implementation of Information Security Policy with reference to this Area

Gap assessment for complying with RBI guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds (Gopalakrishnan Committee recommendations. RBI circular no. RBI/2010-11/494 DBS.CO.ITC.BC.No: 6/31.02.008/2010-11 dated 29.04.2011) with specific reference to Information Security, Cyber frauds.

Application Software (in–house develoepd)

The proposed audit should cover Adherence to business rules in the flow and accuracy in processing, Validations of various data inputs, logical access control and authorization, Exception handling and logging etc. in general.

Gap assessment for complying with RBI guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds (Gopalakrishnan Committee recommendations. RBI circular no. RBI/2010-11/494 DBS.CO.ITC.BC.No: 6/31.02.008/2010-11 dated 29.04.2011) with specific reference to this Area.

Annexure ï A

Documents Establishing SP's Pre-Qualification Criteria

The Bidder shall furnish, as part of his bid documents establishing the Bidderôs eligibility.

2.8.1 The SP should be in existence for a period of at least 3 years	Annexure -1
2.8.2 The SP should have a minimum total turnover of Rs. 50 lacs each for the last two years.	Annexure -2 Audited Balance Sheets and other Financial Statements for 2010-11& 2011-12
2.8.3 The SP should be a profit making entity in the last 2 years	Annexure -3 Audited Balance Sheets and other Financial Statements for 2010-11& 2011-12
2.8.4 The SP should be empanelled by CERT-In (Indian Computer Emergency Response Team) for the period valid up to 31.03.2015	Annexure -4
2.8.5 The SP should have a pool of resources (minimum 5 professionals) who possess certifications such as: CISA/ CISSP/ CISM/DISA	Annexure -5
2.8.6 The SP should have conducted at least one audit of DC in any Scheduled Commercial Banks having not less than 500 branches in India.	Annexure-6 Copies of Purchase Orders & Sign off documents in support of implementation
2.8.7 Existing Dena Bankôs CBS consultant/supplier is not eligible to participate in the audit.	Annexure-7
2.8.8 The SP should be a legal entity in India and have its registered Office in India.	Annexure-8
2.8.9 The SP should not have been black ï listed by any Public Sector, RBI or IBA or any other regulator / statutory body.	Annexure-9
2.8.10 The SP should not have audited area/ areas during the two previous audits of our Bank.	Annexure-10

Self evaluation by the bidder:

Parameter	Marks
No. of audits of DC, 8 marks for each different Bank (max = 16)	
No. of audits of CBS Finacle, 5 marks for each different Bank (max = 10)	
No of professionals with qualifications such as CISA/CISSP/CISM/DISA in SPôs muster roll. 1 mark for 1 employee (max = 9)	
No of auditors with qualifications such as CISA/CISSP/CISM/DISA and audit experience in CBS ï Finacle (team deployed for DCA of our Bank: 10 mark for 1 such auditor) (max = 20)	
Total Mark (out of 55)	

The Checklist for the daily audit of area (DCA) is enclosed as Annexure ï A1 with 24 + ____ check points.

Annexure ï B

The price offered to the Bank must be in Indian Rupees, inclusive of all taxes and service tax will be extra. Unit fee quoted for first year and second year as F1 and S1 respectively for the audit area (DCA) paid on submission the respective report. If the Bank decides to get audited 1 / 3 days per week, the monthly fees will be calculated on the basis of FD1 / SD1 only for the area-DCA.

Table-1:

Area	Details of area for audit	Frequency of reporting	Unit fee / report (F)	Unit fee / report (S)
DCA	Data Centre ï Continuous ï on a daily basis (Monday to Saturday excluding Bank holidays)	Monthly	(F1)	(S1)
DCA	One day audit	Daily	(FD1)	(SD1)
VAPT	VAPT	Quarterly	(F2)	(S2)
DRS	DRS site ï Bangalore	Quarterly	(F3)	(S3)
NDR	NDR ï Mumbai	Quarterly	(F4)	(S4)
SRP	Short Range IT Plans	Quarterly		
NET	Network Management	Half yearly	(F5)	(S5)
ATM	ATM, Internet Banking / Mobile Banking / IT Products	Half yearly	(F6)	(S6)
PSW	Acquisition and Implementation of Packaged Software	Half yearly per package	(F7)	(S7)
ISW	Development of Software in-house and outsourced	Half yearly per software	(F8)	(S8)
OAI	Audit of Outsourcing Arrangements (all IT related services)	Yearly	(F9)	(S9)
ISS	IS Security Policy	Yearly	(F10)	(S10)
ISA	IS Audit Guidelines & Checklist	Yearly		

Table-2:

Area	Area	First year fees (F)	Second year fees (S)	Total fees (F + S)
1	DCA	(F1 x 12)	(S1 x 12)	DCA-1
2	VAPT	(F2 x 4)	(S2 x 4)	VAPT-234
3	DRS	(F3 x 4)	(S3 x 4)	
4	NDR & SRP	(F4 x 4)	(S4 x 4)	
5	NET	(F5 x 2)	(S5 x 2)	NET-56
6	ATM	(F6 x 2)	(S6 x 2)	
7	PSW	(F7 x 1)	(S7 x 1)	PSW-78
8	ISW	(F8 x 1)	(S8 x 1)	
9	OAI	(F9 x 1)	(S9 x 1)	OAI-9
10	ISS & ISA	(F10 x 1)	(S10 x 1)	ISS-10
			2 years fees, total Rs.	(T1)
			Per day fees (FD1 + SD1) / 2 Rs.	DCA-0 (T2)
			Grand total (T1 + T2) Rs.	(GT)

* CFs: Comparable Fees ï DCA-1,VAPT-234, NET-56, PSW-78, OAI-9, ISS-10, DCA-0

Annexure ï C

Covering letter format

Date: _____2012
Offer Reference No.:_____

To:

The Asst. General Manager
Dena Bank HO.
Inspection & Internal Audit Dept.
4th Floor, 17-Horniman Circle
Fort, Mumbai – 400001.

Dear Sir,

Tender Ref: _____

Dated this _____ day of _____2012

Signature: _____
(in the Capacity of:) _____

Duly authorized to sign the offer for and on behalf of
_____

Annexure ï D

Deviation / No deviation certificate

This is to certify that we accept all the terms and conditions as mentioned in your RFP (ref:) for the Continuous IS Audit of Data Centre and Project Office 2013.

Slno.	Term/Clause ref.no	Description in short	Remarks

Signature: _____
(in the Capacity of:) _____

Duly authorized to sign the offer for and on behalf of
_____

********** END OF RFP **********