Cent Bank Home Finance Limited (CBHFL) invites application for empanelment of Information System Auditor (IS Auditor)

Audit Firm (Proprietorship, Partnership, LLP, Company etc.) which is empanelled with 'CERT-In' and has at least 5 years of Information System Audit (IS Audit) experience post registration with CERT-In can apply.

Application needs to be made in the format enclosed herewith (Application Format for IS Auditor).

Application can be submitted by hand delivery at our corporate office at Mumbai (address mentioned below).

Application must reach by 15/09/2023 (till working hours) to the address mentioned below:

Cent Bank Home Finance Limited
Audit Department
Central Bank of India Mumbai Main Office Building,
6th Floor, M.G. Road, Fort, Flora Fountain,
Hutatma Chowk, Mumbai-400 023

Schedule of Events			
Sl. No.	Description	Date	Time
1	Bid Submission Start Date	19 August 2023	11:00 hrs.
2	Bid Submission End Date	15 September 2023	Till working hours
3	Bid Opening Date	18 September 2023	11:00 hrs.

Other Terms:

1) Bid has to be submitted in sealed envelope. There will be 2 (two) stages for evaluation process - Technical evaluation and Commercial evaluation. Passing score in technical evaluation is 60% overall and 50% in each of the groups. Commercials (Audit fees) will be considered only if the Auditing organization is qualified in technical evaluation. Therefore, organization must quote their fees separately in a sealed envelope. Evaluation will be done by a team in presence of Committee of Executives (CoE). Decision of the Company in this regard is final.

Technical evaluation			
Group	**Parameters**	**Max. Score**	**Scoring method**
A	No. of Bank / NBFC / HFC where IS Audit has been done by Auditing organization (Applicant) in last 5 years	20	1) 20 marks - if No. is 4 or more 2) 15 marks - if No. is 3 3) 10 marks - if No. is 2 4) 5 marks - if No. is 1
B	No. of permanent employees on the payroll of Auditing organization who hold professional certifications such as CISA / CEH / CISSP / CISM etc. and will be deployed for Audit	20	1) 20 marks - if No. is 4 or more 2) 15 marks - if No. is 3 3) 10 marks - if No. is 2 4) 5 marks - if No. is 1

C	No. of Audit done in area of Data Migration in last 5 years	20	1) 20 marks - if No. is 4 or more 2) 15 marks - if No. is 3 3) 10 marks - if No. is 2 4) 5 marks - if No. is 1
D	No. of Audit done in area of Change Management (change from Old IT Applications to New IT Applications) in last 5 years	10	1) 10 marks - if No. is 2 or more 2) 5 marks - if No. is 1
E	No. of Audit done in area of New System Implementation in last 5 years	20	1) 20 marks - if No. is 4 or more 2) 15 marks - if No. is 3 3) 10 marks - if No. is 2 4) 5 marks - if No. is 1
F	No. of Audit done in last 5 years in following areas (5 marks for each type of audit) 1) Data Base Administration / Management 2) Cloud Security 3) Application Audit 4) IT Security 5) Cyber Security 6) Network Audit 7) VA/PT 8) IT Governance (Policy/process etc.) 9) Automated Data Flow (ADF) prescribed by NHB / RBI 10) Regulatory compliance	50 (Max.)	Scoring of 5 irrespective of No. of audit in same category
Passing marks is 50% in each category and 60% overall (Min. Overall score must be 84 and min. score of Group A, B, C, D, E & F must be 10, 10, 10, 5, 10 & 25 respectively.			

2) Representatives of Bidder may be present during opening of Bid at Corporate Office at Mumbai. However, Bids will be opened even in the absence of any or all of the bidders. The shortlisted firm as IS Auditor for the Company (CBHFL) will be communicated.

3) Mere submission of application and / or empanelment, does not, in any way constitute any right for allotment of any audit work from the Company (CBHFL). Allotment of work is the sole discretion of the Company and work will be allotted as and when need arises.
4) Company reserves the right to cancel / modify / terminate the appointment at any point of time if performance is found to be not satisfactory for the reasons such as non-deployment of qualified manpower, quality of audit, slow progress of audit etc.
5) In case of any addendum and corrigendum, same will be published on website only.
6) Audit firm will ensure that only qualified persons with adequate experience and expertise are deployed for the job after conducting necessary due diligence / background verification. Company may check the qualification of each of the auditors deployed by IS Audit firm for audit of the Company (CBHFL).
7) Audit Firm which will be shortlisted for IS Audit needs to execute Non-Disclosure Agreement (NDS).
8) Permission needs to be obtained before testing of Denial of Service (DoS) or similar other tests.
9) Audit related data needs to be stored only on systems located in India with adequate safeguards.
10) Company may set other terms & conditions at any point of time but before submission of IS Audit report in mutual agreement between Company (CBHFL) & IS Audit Firm shortlisted for job.
11) Audit Documentation: Audit evidence / information gathered by Audit Firm during audit needs to be appropriately documented and organized to support findings and conclusions of the Audit firm.. Documents which will form part of Audit documentation are – *Audit Report*, *Test Reports & working notes*, *Evidence / Information gathered*, *Snapshot reports*, *mail correspondence*, *any other document / information which is relevant to finding / observation*.
12) Audit Rating: Based on the criticality of the IT system / process and observation, rating needs to be done in 3 points scale – High, Medium & Low. Rating needs to be done against each of the parameters besides overall rating. If any of the parameters

mentioned in the scope is not applicable to CBHFL, same needs to be mentioned clearly with reason.

Possible resolution for the problem (suggestion / recommendation) needs to be mentioned in IS Audit report.

13) Audit needs to be completed and report needs to be submitted within 45 days from the date of execution of Non-Disclosure Agreement (NDS). Committee of Executives (CoE) may extend time if 'CoE' thinks fit.
14) Audit needs to be done independently with adequate care & diligence and findings / observations need to be supported by evidences, failing which may attract penalty up to the tune of the fees agreed upon for the audit.
15) Description & scope of work mentioned here is indicative and can be changed / modified at any point of time but before submission of IS Audit report by the Company (CBHFL) in mutually agreeable terms & conditions.

Description & Scope of Work	
Ref. No.	**Description & Scope**
A. Data Migration & Data Administration / Management: Data has been shifted from old system to new system due to change in IT Application / Vendor. IS Audit must comment on the Availability & effectiveness of policy & process & oversight of IT system, Adequacy & Effectiveness of controls, Recommendation for corrective actions for deficiencies on the following:	
1	Data Transfer: Data transferred from Old server (provided by Old Vendor) to New Server (provided by New Vendor).
1.1	*Completeness of Data transfer: Data available in Old server has been transferred completely to New server.*
1.2	*Correctness of Data transfer: Data available in Old server has been transferred to New server correctly.*

1.3	*Verification of data transferred from Old server to New server to ensure completeness & correctness of data so transferred.*
1.4	*Proper storage / archival of Data in New server*
2	Data Security / Management in New Server (provided by New Vendor):
2.1	*Data Confidentiality: Access of Server / data to authorized users only and recording audit trail (User details, Date, Time, Duration of access, Table / Data accessed etc.).*
2.2	*Data Integrity & Authenticity: No modification of data without proper authorization and recording of audit trail and availability of mechanism to ensure data / information remain same from time of its creation till end and throughout its life cycle.*
2.3	*Data Availability: Availability of data / information of any period / interval to authorized users as & when needed and recording of audit trail.*
2.4	*Data Accessibility & Accuracy & Consistency:*
2.4.1	*Data Accessibility: Data / information / Report of any period / interval is accessible to User at front end of New IT Application system.*
2.4.2	*Data Accuracy: Data / Information of any period / interval generated from New IT Application system is accurate and same in all reports.*
2.4.3	*Data Consistency: Data / Information / Report of any period / interval generated from New IT Application system is same irrespective of point of generation.*
3	Data Centre Management including Data Back Up:
3.1	*Primary Data Centre / Server*
3.2	*Back Up Data Centre / Server*
3.3	*Storage of Data in India*

4	Data Centre Security
4.1	*Physical Security*
4.2	*Logical Security*
5	Any other area / sub-areas IS Auditor thinks fit
B. <u>Change management</u>: Company has shifted its operations from old system to new system. IS Audit must comment on the Availability & effectiveness of policy & process & oversight of IT system, Adequacy & Effectiveness of controls, Recommendation for corrective actions for deficiencies on the following:	
6	<u>Completeness of delivery</u>: Whether Vendor has delivered all IT Applications / system / sub-system, Cloud services, Networking services etc. with reference to the delivery agreed upon in Agreement / RFP.
7	<u>Correctness of delivery</u>: Whether the delivered IT Applications / system / sub-system, Cloud services, Networking services etc. are as per specification / requirement with reference to the delivery agreed upon in Agreement / RFP.
8	New System Implementation
8.1	*<u>Business Process Mapping</u>: Availability of signed documents showing steps from start to end of Business processes with logic to be followed / set in the IT application system.*
8.2	*<u>Software Testing (Script, Test Result, Confirmation / Sign Off)</u>: Detailed step-by-step information about the system transactions that should be performed to validate the application / system under test with 'Expected result', 'Actual result' and sign off / confirmation / Certification by 'Testing team'. This needs to be ensured in the tests mentioned below (8.2.1 to 8.2.8).*

8.2.1	*Unit Testing including White Box Testing: Verification / Testing of internal logic, program source code, design document etc. by Vendor's Testing Team for each of the functionality / module of software to ensure conformance to user requirement.*
8.2.2	*Black Box Testing: Verification / Testing of program inputs and output of every functionality / module of software with respect to user requirements and standard by Vendor's Testing Team.*
8.2.3	*Integration Testing / System Testing: Verification / Testing of each module / system and its compatibility & integration with other modules by Vendor's Testing Team.*
8.2.4	*Volume & Stress Testing: Verification / Testing of module / system capability to handle multiple users accessing a particular module and/or different modules at same time by Vendor's Testing Team.*
8.2.5	*Security Testing: Verification / Testing on points such as Access privileges, Access rights, DoS, firewall configuration including points like Trapdoors, Salami Technique etc. by Vendor's Testing Team.*
8.2.6	*User Acceptance Testing (UAT): Verification / Testing of each functionality / user requirement of every functionality / module by Testing Team of User Company (CBHFL).*
8.2.7	*Testing by 'Testing Team' of CBHFL: Verification / Testing of "End-to-end" testing of transactions having impact on different modules in system by Testing Team of User Company (CBHFL).*
8.2.8	*Testing by 'End-Users' of CBHFL: Verification / Testing of "End-to-end" testing of transactions having impact on different modules in system by 'End Users' of Company (CBHFL).*
8.3	Sign Off by Competent Authorities & Functions & IT Person/(s) for Go live
8.4	System Implementation / Go live
8.5	Output Monitoring to ensure completeness, correctness & compliance to requirements.
9	Others: Data Processing, Data synchronization, Audit trails, Version control, Patch management, Rollover / Setting of various parameters.

10	Delivery of IT Application with reference to the time agreed upon in Agreement / RFP
11	Billing & Payment with reference to Agreement / RFP
12	Any other area / sub-areas IS Auditor thinks fit

C. Others:

IS Audit must comment on the Availability & effectiveness of policy & process & oversight of IT system, Adequacy & Effectiveness of controls, Recommendation for corrective actions for deficiencies on the following:

13	IT Governance
14	IT Policy including User Management (Id Activation / De-activation, Access right etc.)
15	Information & Cyber Security including VAPT, Internet Protocol Version etc.
15.1	Policy / Organization of Information Security
15.2	Cyber Crisis Management
16	IT Operations
16.1	*LAN administrator has a backup person*
16.2	*LAN administrator monitors the LAN response time, disk storage space, and LAN utilization*
16.3	*LAN administrator is experienced and familiar with operation of the LAN facility.*
17	Business Continuity Planning (BCP) & DR Drill
18	IT Service Outsourcing
19	IT Access Control
20	IT Back-up & Recovery
21	The network has adequately documented backup and recovery procedures / plans / schedules for critical sites.

21.1	*The network has adequately documented backup and recovery procedures / plans / schedules for critical sites.*
21.2	*LAN is supported by an uninterruptible power supply (UPS)*
21.3	*UPS tested in the last year (to test the batteries)*
21.4	*For disaster-recovery purposes, LAN applications have been prioritized and scheduled for recovery based on importance to the operation.*
22	IT Environment Controls (Smoke detection and automatic fire-extinguishing equipment installed for adequate functioning and protection against fire hazards etc)
23	IT Inventory - Asset Management
23.1	*There is a complete inventory of the following: Hardware: Computers, File Servers, Printers, Modems, Switches, Routers, Hubs, etc. Software: all software for each Computer is logged with licenses and serial numbers*
23.2	*There are written procedures for keeping LAN inventory and they identify who (title) is responsible for maintaining the inventory report.*
23.3	*Unused equipment is properly and securely stored.*
24	IT Security
24.1	*Physical Security*
24.2	*Logical Security*
24.3	*Incident Management & Root Cause Analysis (RCA)*
24.4	*Business Impact Analysis*
24.5	*RTO & RPO*
24.6	*IT Risk Assessment*
25	IT Service Agreement and Service provided by Vendor
26	Compliance to various regulatory and statutory requirements (RBI, NHB, CERT-In etc.)

27	IT - Virus Protection
28	Impact of Business / Product decision on system (system compatibility, readiness, control etc. with reference to the Business / Product)
29	Cloud Security & Controls
30	Operational Security
30.1	*Patch Management*
30.2	*Capacity Management*
30.3	*Logs Management*
31	Communication Security
32	User Management
32.1	*User Manual*
32.2	*User Training (Schedule of training, Participants, Duration of Training etc.)*
33	Other areas / activities which IS Auditor thinks fit & appropriate for assessing the efficacy of the system & control of IT of the Company and to conclude whether the present system is resilient to threat or not

Application Format for IS Auditor Cent Bank Home Finance Limited (CBHFL)	
Name of the Auditing organization (Firm)	
Nature of the IS Audit Firm (PSU / Public Co. / Pvt. Co. / Partnership, LLP, Proprietorship etc.)	
Name of Managing Person with Designation	
Date of registration of the firm	
Date of registration with CERT-In	
Address of the firm, Contact No. & E-mail Id of IS Audit firm/company	
Single Point of Contact (Name, Contact No., E-mail Id, Designation)	
No. of Bank / NBFC / HFC where IS Audit has been by Auditing organization (Applicant) in last 5 years	Separate sheet to be attached mentioning Name of Organization, Adress & Contact details of organization, Year of engagement etc. (Necessary documents to be attached also)
No. of Permanent employees on the payroll of IS Auditor who hold professional certifications such as CISA / CEH / CISSP / CISM etc. and will be deployed for audit	Separate sheet to be attached mentioning Name, Year of experience, Qualification, Areas audited etc.
No. of Audit done in area of Data Migration in last 5 years	Separate sheet to be attached mentioning Name of Organization, Adress & Contact details of organization, Year of engagement etc. (Necessary documents to be attached also)

No. of Audit done in area of Change Management (change from Old IT Applications to New IT Applications) in last 5 years	Separate sheet to be attached mentioning Name of Organization, Adress & Contact details of organization, Year of engagement etc. (Necessary documents to be attached also)
No. of Audit done in area of New System Implementation in last 5 years	Separate sheet to be attached mentioning Name of Organization, Adress & Contact details of organization, Year of engagement, Area of audit etc. (Necessary documents to be attached also)
Areas audited by the Firm like Network, IT Security, Cyber Security etc. (refer technical parameters mentioned under F under terms & conditions) in last 5 years	Separate sheet to be attached mentioning Name of Organization, Adress & Contact details of organization, Year of engagement, Area of audit etc. (Necessary documents to be attached also)
Expected Audit Fees	To be quoted in sealed envelope (will be opened only if applicant is technically qualified)

Declaration:

I/We hereby certify that the above information is true and correct to the best of my/our knowledge. I/We understand that CBHFL has right to take any step as it deems fit at any point of time if any of the above information is found to be false or incorrect and / or in case any auditor is found to be guilty of misconduct in professional capacity in some other bank / institution and his name has been circulated/reported by the Indian Banks Association (IBA) / Central Bureau of Investigation (CBI)/ Reserve Bank of India (RBI) / Any other Govt. Agency / Body.

CBHFL may call for additional document / proof in support of any of declarations made above if CBHFL deems fit at any point of time.

Signature of Authorized person of the Firm with Seal & CERT-In Registration Number

Applicant can submit additional relevant information if thinks fit.