

Sl. No	Section and Clause Reference	Page No.	RFP Text	Query	Response to query (to be left blank for company by the vendor)
1	Bidding Process (Three Part Offer):	7	Bid shall have the following 3 (Three) parts; Eligibility conformity, Technical Scope and Commercial proposal. The three parts must be submitted at the same time but in separate sealed covers, giving full particulars, addressed to the Assistant Vice President & Head of IT, Can Fin Homes Ltd, 29/01 – SIR M N Krishna Rao Road, Basavanagudi, BANGALORE – 560 004 and these covers should also indicate name, address and contacts of the bidder submitting the offers.	Kindly confirm whether the bid submission is to be made via email or as a hard copy, and we kindly request you to provide an option for email submission.	Bid shall have the following 3 (Three) parts; Eligibility conformity, Technical Scope and Commercial proposal. The three parts must be submitted at the same time but in separate sealed covers. Hard Copies only. Submission through email will not be considered.
2	EARNEST MONEY	47	5.1. Every BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER while submitting commercial bid, shall deposit an amount as specified in RFP/Tender Documents as Earnest Money, with the BUYER through any of the instruments as detailed in the tender documents.	Kindly confirm the EMD amount and provide the bank details, including the account information and submission procedure, for depositing the EMD.	EMD is not required for this engagement. Kindly refer to the amendment.
3	Timelines, Deliverables & Service Level Agreements (SLAs)	10	The bidder shall align the audit activities with the phase-wise delivery timelines which are currently in progress of the System Integrator (SI) as outlined in the Scope of Work. The overall audit engagement shall be completed with closure of all open items as per the audit findings and as per the concurrence of the Company within a maximum period of three (3) months from the date of completion of the CBS implementation project.	Kindly provide clarity on the total duration of the audit, including the expected start and end dates, along with any key milestones.	The timelines including the expected Start date and the end dates are mentioned in the RFP Clause No. 12(1). Bidder to comply with RFP T&C's.
4	Annexure IV: Scope of Work d) Detailed Scope of Work	24 - 40	General	Kindly clarify whether, as stated in the scope, the requirement is limited to reviewing the reports or if VAPT testing is also expected to be performed.	Yes VAPT testing is also expected. Please refer to Exhibit A Section U Page No. 40
5	Annexure IV: Scope of Work d) Detailed Scope of Work	24 - 40	General	Kindly clarify whether the audit is to be conducted on a sample basis or if any specific audit methodology or approach is required to be followed.	Methodology of the audit is articulated in Scope of work section. The proposed methodology of bidder will also be considered as part of evaluation criteria as mentioned in RFP. Bidder to comply with RFP T&C's to cover entire scope as articulated in RFP document.
6	Annexure IV: Scope of Work d) Detailed Scope of Work	24 - 40	General	Kindly provide additional clarity and detailed information regarding the documents and checklists mentioned for review.	The documents and checklist are relevant to CBS implementation as per scope of RFP-IT-140/2024-2025 dated 26.08.2024.
7	Annexure IV: Scope of Work d) Detailed Scope of Work a) General Audit Section	24	1. Cloud Architecture review for completeness	Kindly clarify which specific cloud platforms (AWS, Azure, GCP, or Private Cloud) fall within the scope of the Cloud Architecture Review, and kindly confirm the number of cloud tenants and microservices included.	AWS Multi Tenant including Microservices.
8	Annexure IV: Scope of Work d) Detailed Scope of Work a) General Audit Section	24	3. Release Checklist Verification	Kindly specify whether the Release Checklist is standardized across all applications or varies by component, and kindly confirm the total number of checklists and approximate number of controls included in scope.	The documents and checklist are relevant to CBS implementation as per scope of RFP-IT-140/2024-2025 dated 26.08.2024.
9	Annexure IV: Scope of Work d) Detailed Scope of Work a) General Audit Section	24	7. Complied as per Outsourcing guidelines. Overall deployment as per guidelines	Kindly clarify whether the reference to "Outsourcing guidelines" pertains to the RBI Outsourcing Guidelines or any other specific regulatory or internal guideline.	It pertains to the RBI Outsourcing Guidelines.
10	Annexure IV: Scope of Work d) Detailed Scope of Work a) General Audit Section	25	14 g) Re-assessment API Audit Report to be provided with closure of all the vulnerabilities observed.	Kindly clarify what the reference to the re-assessment of API audit reports pertains to, as it is mentioned only in the 'Reporting, Support, and Submission of Reports' section and not in the generic audit scope.	Reporting, support and submission of reports is applicable for all points in Generic Audit section.
11	Annexure IV: Scope of Work d) Detailed Scope of Work Exhibit A - A	27	Source Code Assessment (SAST) Source code assessment should be performed for all in- scope applications (including web applications and mobile applications) and API's.	Kindly confirm the number of web applications, mobile applications (separately for Android and iOS), and APIs included in the scope, along with the number of static and dynamic s and the total number of user roles.	CBS implementation as per scope of RFP-IT-140/2024-2025 dated 26.08.2024.
12	Annexure IV: Scope of Work d) Detailed Scope of Work Exhibit A - C	28	Version Management and Release Management Review the application code version and the major/minor changes committed in the version management tool (e.g. SVN, BitBucket, Gitlab etc.)	Kindly confirm the number of code versions or releases that will be made available for review.	CBS implementation as per scope of RFP-IT-140/2024-2025 dated 26.08.2024. Successful bidder will be given additional information.
13	Annexure IV: Scope of Work d) Detailed Scope of Work Exhibit A - D	28	Secure Code Review and Static Application Security Testing (SAST)	Kindly confirm the total number of lines of code (LOC) that will be provided for Source Code Review.	CBS implementation as per scope of RFP-IT-140/2024-2025 dated 26.08.2024. Successful bidder will be given additional information.
14	Annexure IV: Scope of Work d) Detailed Scope of Work Exhibit A - F	29	Network and Device Configuration Review	Kindly specify the total number and types of network and security devices that will be included in the assessment (such as firewalls, switches, routers, WAF, IPS, VPN gateways, wireless controllers, databases etc.).	CBS implementation as per scope of RFP-IT-140/2024-2025 dated 26.08.2024. Successful bidder will be given additional information.
15	Annexure IV: Scope of Work d) Detailed Scope of Work Exhibit A - F	29	Network and Device Configuration Review	Kindly clarify whether the Network and Device Configuration Review will be conducted on a sample basis, and if so, provide the expected sampling percentage.	CBS implementation as per scope of RFP-IT-140/2024-2025 dated 26.08.2024. Successful bidder will be given additional information.

16	Annexure IV: Scope of Work d) Detailed Scope of Work Exhibit A - F	29	Network and Device Configuration Review	Kindly specify which architecture model is being deployed. DC, DR and Head Office locations	Hub & Spoke model.
17	Annexure IV: Scope of Work d) Detailed Scope of Work Exhibit A - M.1	33	a) Check for the 3rd party information security policy. Check for 3rd party information security risks and compliances documentation / reports for open / critical risks and issues.	Please confirm the total number of third-party vendors/suppliers currently engaged by the organization	CBS implementation as per scope of RFP-IT-140/2024-2025 dated 26.08.2024. Successful bidder will be given additional information.
18	Annexure IV: Scope of Work d) Detailed Scope of Work Exhibit A - O.1	36	Penetration Testing Scope and Coverage (Review the network penetration testing policy to determine the periodicity and coverage of network penetration tests. Review the past penetration testing reports to determine whether penetration tests covered the critical assets and network segments. Review whether automated and manual penetration testing was performed.)	Kindly confirm how many past penetration testing reports (e.g., previous 1 cycle, 2 cycles, or more) are required to be reviewed. as part of the audit scope	This is a greenfield implementation and bidder to abide by Scope of Work as per T&C's of the RFP.
19	Annexure X: Bill Of Materials	44	Bill of Material/ Price Schedule	Kindly clarify the distinction between Milestone 1, defined as the Final Audit Report, and Milestone 2, defined as the Final Audit Report completed with observations addressed, and specify what activities or deliverables differentiate the two milestones.	Milestone 1 & 2 definitions corresponds to the sections 42 (d) a, b and c of the scope of work.
20	General	General	General	A brief on the CBS product and version that is being implemented, and clarification if the same is a first time implementation or a migration activity.	This a greenfield development and the scope is as per the RFP-IT-140/2024-2025 dated 26.08.2024.The successful bidder will be given additional information.
21	Timelines, Deliverables & Service Level Agreements (SLAs)	10	The bidder shall align the audit activities with the phase-wise delivery timelines which are currently in progress of the System Integrator (SI) as outlined in the Scope of Work. The overall audit engagement shall be completed with closure of all open items as per the audit findings and as per the concurrence of the Company within a maximum period of three (3) months from the date of completion of the CBS implementation project.	Expected timeline of completion of CBS Implementation project at CanFin - is it completed or in progress. As the timeline for review is mentioned as 3 months from Completion of implementation - we would require this information for us to evaluate. Considering the comprehensive scope of coverage for the audit - request to consider extension of the timeline to 5 months.	The timelines including the expected Start date and the end dates are mentioned in the RFP Clause No. 12(1). Bidder to comply with RFP T&C's.
22	ANNEXURE - VI: Scope of Work	23	For each item listed in the table below, the bidder must indicate the number of audit engagements undertaken and may include any relevant remarks or references demonstrating their experience. Supporting documents or client references may be requested during the evaluation process.	Is experience to be provided for all 25 areas. Is there a time limit in specifying the past experience - like last 5 years or 10 years, etc. Request to include a evaluation based on grading.	Based on the actual experience of the bidder in all the areas. No limit in specifying past experience. Please comply with the RFP T&C's.
23	Exhibit A	27	Source Code Assessment (SAST) Source code assessment should be performed for all in- scope applications (including web applications and mobile applications) and API's, Application Testing (SAST)	Request to kindly provide a list and count of such in-scope items for us to arrive at the effort.	CBS implementation as per scope of RFP-IT-140/2024-2025 dated 26.08.2024.
24	Exhibit A - J	31	API Standards: API Specifications: Reviewing APIs against OpenAPI (Swagger) specifications.	Request to kindly provide a list and count of such in-scope items for us to arrive at the effort.	CBS implementation as per scope of RFP-IT-140/2024-2025 dated 26.08.2024.
25	Exhibit A - U	40	Security Assessment: ☐ Vulnerability Assessment & Penetration Testing ☐ API Security Review ☐ Configuration Review o Server Hardening (OS settings, unnecessary services disabled) o Firewall Rules (ingress/egress, least privilege) o Web Application Firewall (WAF) settings o Database Security (encryption, access control) o Cloud Configuration (security groups, buckets, IAM roles, EC2 instances) ☐ Web Application Security Testing ☐ Mobile Application Security Testing ☐ Container & Microservices Security Review ☐ ITGC controls (covering access control, change management, backup & recovery, and IT operations) ☐ Regulatory compliances ☐ Mobile Application Management (MAM) and Mobile Device Management (MDM)	Request to kindly provide a list and count of such in-scope items for us to arrive at the effort.	CBS implementation as per scope of RFP-IT-140/2024-2025 dated 26.08.2024.
26	ANNEXURE - VI: Scope of Work	22	Scope of work for performing CBS Implementation audit: The company is on Digital Transformation exercise. Currently System Integrator is engaged and implementation is in progress in multiple phases as mentioned in the below table.	In delivery audit - is the expectation to check entire CBS configuration - along with all the other delivery channels as mentioned in table in page	This is greenfield implementation. Entire CBS is expected to be audited. Bidder to comply with RFP T&C's.

27	Bid detail Table S.N.6	2	Physical Pre-bid meeting will be held on 25.11.2025 at 16:00 hrs.	Please allow to join online also	Link will be shared.
28	Evaluation Criteria 1.B	8	Past Experience of conducting Infrastructure, Application, and Security Audits of CBS or similar large-scale IT systems in BFSI sector organizations / NBFCs / Scheduled Commercial Banks / Government Departments / PSU organizations / Housing Finance Companies in India. 3 projects in the last 2 years (5 marks each)	Please allow to have 3 projects in last 5 years	Please comply with RFP T&C's.
29	S.N12.II	10	The bidder shall align the audit activities with the phase-wise delivery timelines which are currently in progress of the System Integrator (SI) as outlined in the Scope of Work. The overall audit engagement shall be completed with closure of all open items as per the audit findings and as per the concurrence of the Company within a maximum period of three (3) months from the date of completion of the CBS implementation project.	By when CBS implementation will complete	Bidders to align their audit in a phased manner as per the Drops mentioned in the RFP. And close entire audit before 3 months post go live.
30	Table 1 Point 2,3 and 4 Table 2 Point 2 Proposed Audit Evaluation Matrix	22	Loan Management System including Collection Module. Performance & scalability Matrix	We are are mainly an Information Security and Information Risk Management Organisation. Our main experiences are on info sec. Hope the credential will hold merit for the intended audit.	The bidders responses will be evaluated as per the T&C's of the RFP including eligibility criteria,credentials, technical solution, commercials etc. for consideration in the bidding process.
31	Eligibility Point No 2	18	The Bidder should have conducted Infrastructure, Application, and Security audits of Core Business Solutions (CBS) or similar large scale IT systems at least once during the period	Please allow for Core Banking Solution experience to be considered	The Bidder should have conducted Infrastructure, Application, and Security audits of Core Business Solutions (CBS) or similar large-scale IT systems at least once during the period from 01/04/2023 to 31/03/2025 in BFSI sector organizations / NBFCs / Scheduled Commercial Banks / Government Departments / PSUs / Housing Finance Companies in India or in any listed company in India
32	a) Generic Audit Section, 4	24	DC DR set up document review for completeness	Please clarify if your Data Centre (DC) and Disaster Recovery (DR) infrastructures are currently hosted on-premises, on the cloud (either fully or partially), or deployed in a hybrid model?	Fully on AWS cloud
33	a) Generic Audit Section, 13 c) Security Audit Section, A 1.1	25, 27	The auditor should be CERT-In-emplanelled and, in case of application hosted on cloud, the auditor and should have the capability for carrying out cloud security audit as per the empanelment details available on CERT-In's website. Identify the application testing scope and review the testing methodology.	Could you please provide clarification on the total number of in-scope applications that are required to be covered as part of this project	This a greenfield development and the scope is as per the RFP-IT-140/2024-2025 dated 26.08.2024. Application details are already mentioned in Annexure VI of the scope of work of the RFP.
34	39. ANNEXURE -III: Pre-Qualification Criteria (Eligibility) Declaration	18	The Bidder should have conducted Infrastructure, Application, and Security audits of Core Business Solutions (CBS) or similar large scale IT systems at least once during the period from 01/04/2023 to 31/03/2025 in BFSI sector organizations / NBFCs / Scheduled Commercial Banks / Government Departments / PSUs / Housing Finance Companies in India or in any listed company in India.	We kindly request that the experience period be revised from the current 2-year window (01/04/2023 to 31/03/2025) to a 5-year period, allowing bidders with relevant engagements completed in the last 5 years to be considered	Please comply with RFP T & C's.
35	42. ANNEXURE - VI: Scope of Work	22	a) Scope of work for performing CBS Implementation audit: The company is on Digital Transformation exercise. Currently System Integrator is engaged and implementation is in progress in multiple phases as mentioned in the below table.	The RFP outlines Drop 1, Drop 2, and Drop 3 for CBS implementation but does not specify timelines. Please clarify the tentative start/end dates and key milestones for each drop.	Drop 1, Drop 2 and Drop 3 implementation are currently in progress. This audit needs to be commenced on the basis of Go-live applications in phased manner.
36	8. Evaluation Criterion 1. A	8	Experience in conducting Infrastructure, Application, and Security Audits of Core Business Solutions (CBS) or similar large-scale IT systems in Banking/Financial Institutions/NBFCs/Housing Finance Companies or other Critical Infrastructure Institutions: More than 3 years – 15 marks >2 years and ≤3 years – 10 marks ≥1 year and ≤2 years – 05 marks Less than 1 year – 0 marks	Could you please provide clarification on how 'more than 3 years of experience' will be evaluated. Would a 2021 PO be sufficient to qualify for the 15 marks, or is the requirement based on the cumulative number of years of relevant audit engagements completed?	Please comply with RFP T&C's.
37	-	-	-	Could you please provide clarification on the tentative timelines for the overall process, and expected completion dates?	Drop 1, Drop 2 and Drop 3 implementation are currently in progress. This audit needs to be commenced on the basis of Go-live applications in phased manner.
38	46. ANNEXURE – X – Bill of Material	44		Could you please clarify what Group A, Group B, and Group C represent in the Bill of Material, and the basis on which these groupings have been defined?	Group A, Group B and Group C corresponds to Drop 1, Drop 2 and Drop 3 mentioned in the scope of work respectively. BOM is applicable for consolidated scope.
39	Criteria		PO copies from the clients	As part of credentials, it is mentioned that POs are to be submitted. Can we submit ELs as well?	Along with PO copies, a project completion certificate or client engagement letter will also be acceptable for credential evaluation.
40	12. Timelines, Deliverables & Service Level Agreements (SLAs) 1. Project Timeline	10	The objective of this engagement is to assess the CBS infrastructure, application, and security framework with respect to performance, configuration, data integrity, access controls, cybersecurity, compliance, and alignment with industry best practices.	We understand that the asset baselines and the complete asset inventory will be provided and are to be considered as part of the scope. Please confirm Furthermore, for the assets and configuration which have not been completed as part of the implementation, how do we consider these assets coverage in scope. Need clarity	Successful bidder will be given additional information on various CBS components. SI partner is expected to complete the CBS implementation including all the components as per the scope of work mentioned in the **RFP IT/140/2024-25. Bidder is expected to comprehensively audit as per the scope of this RFP.
41	12. Timelines, Deliverables & Service Level Agreements (SLAs) 1. Project Timeline	10	The bidder shall align the audit activities with the phase-wise delivery timelines which are currently in progress of the System Integrator (SI) as outlined in the Scope of Work.	We understand that the implementation is in progress by the SI. Is this a new implementation or migration / Upgrade from existing system. Please Clarify	It's predominantly a greenfield CBS implementation. For further details please refer to the **RFP IT/140/2024-25.

42	12. Timelines, Deliverables & Service Level Agreements (SLAs) I. Project Timeline	10	The bidder shall align the audit activities with the phase-wise delivery timelines which are currently in progress of the System Integrator (SI) as outlined in the Scope of Work.	What are the delivery timelines which are currently in progress of the System Integrator (SI). Need details to align our timelines and activities accordingly	Drop 1, Drop 2 and Drop 3 implementation are currently in progress. Bidder needs to start the project as soon as the PO is issued and audit should be completed within 3 months post CBS implementation Go-Live.
43	12. Timelines, Deliverables & Service Level Agreements (SLAs) I. Project Timeline	10	The overall audit engagement shall be completed with closure of all open items as per the audit findings and as per the concurrence of the Company within a maximum period of three (3) months from the date of completion of the CBS implementation project.	We understand that the closure of the open audit findings will not be our responsibility. Please confirm	As per the scope of the RFP, relevant evidences, along with two hard copies reflecting the closure or resolution of audit findings (with screenshots wherever applicable), should be provided to CFHL post obtaining sign-off from the relevant stakeholders, as aligned with CFHL.
44	12. Timelines, Deliverables & Service Level Agreements (SLAs) I. Project Timeline	10	The overall audit engagement shall be completed with closure of all open items as per the audit findings and as per the concurrence of the Company within a maximum period of three (3) months from the date of completion of the CBS implementation project.	We understand that we will not be responsible for closure of open audit findings for completion timelines going beyond 3 months	Audit has to be completed within 3 months post entire CBS implementation. Audit activity can be initiated by the successful bidder as soon as PO is issued. Hence audit activity will overlap with CBS implementation and to be aligned with dropwise implementation plan. All the audit findings have to be closed before 3 months after go-live of CBS implementation in consultation with the relevant stakeholders.
45	13. Payment Terms:	11	Payment Milestone 30% of the milestone payment will be made post fixing of the audit finding & sign off is received from the relevant stake holders in phase manner as referred in the commercial proposal.	Since we will not be responsible for fixing and closure of the open audit findings, will this affect the payment incase the closure is beyond 3 months. Need clarity	Audit has to be completed within 3 months post entire CBS implementation. Audit activity can be initiated by the successful bidder as soon as PO is issued. Hence audit activity will overlap with CBS implementation and to be aligned with dropwise implementation plan. All the audit findings have to be closed before 3 months after go-live of CBS implementation in consultation with the relevant stakeholders.
46	Proposed Audit Evaluation Matrix	23	These parameters will serve as the basis for evaluation to ensure that the system complies with the defined performance, security, and regulatory benchmarks. i. Performance & scalability Matrix ii. Availability & fault tolerance iii. Security & Access Control iv. Robustness & maturity v. Confirmation to standards & interoperability	We understand that the performance parameters, sizing and solution design must have been prepared by SI and will be available to us for the evaluation of these parameters. Please confirm. Furthermore we understand that relevant performance, availability etc, reports will be made available to us during the audit. Please confirm	Successful bidder will be given additional information about the CBS implementation.
47	Proposed Audit Evaluation Matrix	24	The selected bidder shall clarify the integration mechanism between the CBS and the SaaS applications, including details on the interfaces, data exchange methods (such as APIs or middleware), and the security controls governing the interaction.	We will need i) details of the on-premise (DC, DR and NDR sites) locations and ii) list of SaaS applications, along with the service provider / OEM, to be covered as part of identifying the integration mechanism.	DC and DR will be on AWS Cloud with a combination of SaaS, PaaS and hosted application on cloud. Other relevant details and information will be shared with the successful bidder on need basis.
48	b) Methodology	24	Conduct testing as per Scope of work, Evaluate and submit preliminary reports on findings and submission of final report.	We understand that "conduct testing" means that security and vulnerability testing, and not the application functional testing or any other testing. Please clarify incase anything apart from the above is to be covered as part of testing.	The testing activities are clearly mentioned as part of the scope of the RFP. Kindly comply by RFP T&Cs.
49	a) Generic Audit Section	24	DC DR set up document review for completeness Cloud infra document review for completeness Environment Setup as per architecture doc CBS component Discovery and Inventory:	We understand that the completeness of these documents are to be done against a baseline document (e.g High / Low Level Design or technical solution documents). Please confirm Moreover we will not be responsible for updating / modifying any of these documents. Please confirm	Successful bidder will not be modifying the documentation deliverables shared by SI partner. These documents can be considered for audit purpose.
50		24	Identify all CBS components getting implemented. Documenting components with details. Mapping component dependencies and interactions.	We assume that SI will be performing and documenting the component discovery and Inventory. We will review these documents for completeness and accuracy. Please confirm	Yes
51	b) Delivery Audit Section	26	To verify that all project documents, deliverables, and reports have been formally submitted by the System Integrator (SI) as per contractual obligations.	We assume that the document delivery contractual obligations will be shared to verify the completeness	Successful bidder will be given additional information about the CBS implementation.
52	Annexure-VI - Security Scope - Vulnerability, Threat & Risk Assessment	23-24	Assessment of vulnerabilities, threats, risks in hardware, applications, APIs, configurations, interfaces & security components.	Confirm whether VTR assessment is limited to CBS landscape or includes broader enterprise IT components (AD, DLP, SOC, SD-WAN, etc.).	The complete CBS implementation scope can be referred in Annexure VI of the RFP and also refer in detail scope in master RFP-**RFP IT/140/2024-25. The scope of the audit is complete CBS implementation.
53	Annexure-VI - Security Scope - Vulnerability, Threat & Risk Assessment	23-24	Assessment of vulnerabilities, threats, risks in hardware, applications, APIs, configurations, interfaces & security components.	Please share number of applications along with Sizing for vulnerability assessment	The complete CBS implementation scope can be referred in Annexure VI of the RFP and also refer in detail scope in master RFP-**RFP IT/140/2024-25. The scope of the audit is complete CBS implementation.
54	Annexure-VI - Security Scope - Vulnerability, Threat & Risk Assessment	23-24	Assessment of vulnerabilities, threats, risks in hardware, applications, APIs, configurations, interfaces & security components.	Please share number of IP addresses for vulnerability assessment	Successful bidder will be given additional information about the CBS implementation.
55	SaaS Integration Security Requirements	24	Bidder to explain integration mechanism and security controls for SaaS integrations.	Please provide existing list of security controls for SaaS integration	Successful bidder will be given additional information about the CBS implementation.
56	Exhibit A - Source Code Assessment (SAST)	28-29	Source code assessment for all in-scope applications including APIs.	Confirm whether CBS application source code will be provided. If not, please clarify acceptable alternatives (design review/white-box testing).	Relevant information to comply with the RFP T&Cs will be provided to the successful bidder.
57	Exhibit A - Secure Development / Environment Separation	28-29	Check whether dev, staging and production environments are separate.	Confirm access availability for Dev/SIT/UAT/Pre-Prod/Prod environments	SI partner will facilitate the relevant access in coordination with security guidelines to the auditors to accomplish the audit work as applicable with relevant justification wherever necessary.
58	Exhibit A - Network Vulnerability Assessment	28-29	Review architecture, segmentation, firewall/WAF/IPS/DDoS, patching.	Request network asset inventory, IP ranges, cloud VPC/VNET architecture, and segmentation map to estimate VA effort.	Successful bidder will be given additional information about the CBS implementation.
59	Exhibit A - Asset Inventory Requirement	29	Check existence of updated inventory of computers, network devices, software, users, patching, AMC etc.	Clarify whether auditor must create this inventory or only validate SI/CFHL-maintained inventories.	SI Partner will facilitate the same.
60	Exhibit A - Database Security Assessment	37	Review encryption, MFA, DAM, SIEM integration, patching.	Confirm DB technologies in scope (Oracle/PostgreSQL/MS SQL etc.) and whether read-only DB access & DAM/SIEM logs will be provided.	Yes. Majority is DB technologies used are PostgreSQL/MS SQL.
61	Exhibit A - Application Security Testing	34-36	Perform OWASP/CERT-In testing on Web, Mobile, APIs.	Request total count of Web apps, mobile apps, APIs, and internal portals to size security testing.	Successful bidder will be given additional information about the CBS implementation.
62	Aadhaar Security Compliance	40	Aadhaar Data Vault, HSM key management, UIDAI standards.	Confirm whether CBS stores/processes Aadhaar data and whether Aadhaar Data Vault is already implemented by SI.	Yes. For additional information on SI scope of work please refer to **RFP IT/140/2024-25.
63	IAM / PIM / PAM Controls Review	40-41	Review IAM, privileged access, reconciliation, SSO/MFA.	Please specify IAM/PAM tools used (AD, Azure AD, Okta, CyberArk, etc.) and availability of privileged access logs.	Successful bidder will be given additional information about the CBS implementation.
64	Security Operations Center (SOC) Review	39	Check SIEM correlation rules, device integration, UEBA, TI.	Request list of integrated devices, SIEM technology (Qradar/Splunk/Sentinel/etc.), and current use-case coverage.	Successful bidder will be given additional information about the CBS implementation.

65	Log Retention Requirements	31	Logs must be retained in India for 180 days.	Confirm whether logs are already retained for 180 days within India infrastructure and whether read-only access will be provided.	Successful bidder will be given additional information about the CBS implementation. SI partner will facilitate the relevant access in co-ordination with security guidelines to the auditors to accomplish the audit work as applicable with relevant justification wherever necessary.
66	Cloud Security Audit Requirement	25	Auditor must be CERT-In empanelled & capable of cloud audit.	Specify cloud provider(s) (AWS/Azure/GCP), services used, number of accounts/subscriptions, and whether cloud architecture will be shared.	AWS, Successful Bidder will be given additional information.
67	ITGC Controls Review	40	Covers IT operations, backup, change, access management.	Clarify whether full ITGC testing is expected or only validation of SI's ITGC documentation and controls.	ITGC controls are to be assessed as part of the security assessment.
68	API Security Testing	34-36	API Whitelisting, OWASP API Top 10, TLS checks.	Request number of internal, external, partner APIs and details of API Gateway (Apigee/Kong/AWS/Azure).	Successful bidder will be given additional information about the CBS implementation.
69	DR/Backup/Archival Security Review	31	Review access to logs, backup, archival processes.	Please specify backup solution (Veeam/NetBackup/Commvault/etc.) and availability of DR drill evidence for review.	AWS native backup solutions are in place and DR evidences can be obtained in coordination with SI partner.
70	Interfaces & Integration Security	24	Assessment of integration security between CBS & external systems.	Request list of all interfaces (LOS, LMS, DMS, Aadhaar, HRMS, Payment systems, etc.) with data-flow and authentication methods.	Successful bidder will be given additional information about the CBS implementation.
71	Evidence Requirements	24	Vendor must share logs, screenshots, evidence for vulnerabilities reported.	Clarify whether SI will provide required screenshots/configuration evidence to support reproduction of vulnerabilities.	SI partner will facilitate the relevant access in co-ordination with security guidelines to the auditors to accomplish the audit work as applicable with relevant justification wherever necessary.
72	Re-assessment Scope	26	Re-assessment API audit report with closure of vulnerabilities.	Confirm whether re-assessment is limited to APIs or includes whole scope (Web/Mobile/Infra/Cloud/etc.).	For closure of the milestone relevant evidences along with two hard copies reflecting the closure or resolution of audit findings (with screenshots wherever applicable), should be provided to CFHL post obtaining sign-off from the relevant stakeholders, as aligned with CFHL. The activities to be performed by auditors to accomplish the milestone is expected as per RFP T&C's.
73	Tools for Security Testing	24	"Only licensed version of reputed tools should be used."	Confirm whether CFHL will provide access to tools like SIEM, WAF, DAM, EDR, CSPM, or auditor must use its own toolset.	SI partner will facilitate the relevant access in co-ordination with security guidelines to the auditors to accomplish the audit work as applicable with relevant justification wherever necessary.
74	Log Storage & Access	31	Logs must be stored within Indian jurisdiction.	Confirm whether cloud log storage is allowed if region is India, and whether any additional CERT-In directives apply.	Successful bidder will be given additional information about the CBS implementation.
75	Penetration Testing Constraints	34-36	Application security testing including potential destructive tests.	Confirm whether destructive testing (DoS, brute force stress, fuzzing) is permitted and required test window approvals.	Successful bidder will be given additional information about the CBS implementation.
76	Privileged Access Review	40-41	Review privileged access, segregation of duties.	Confirm whether PAM session recordings or screenshots will be accepted in place of direct console access.	Yes. Successful bidder will be given additional information about the CBS implementation.
77	Data Protection (DPDP Act 2023)	40	Data protection, DPIA, consent, encryption.	Clarify whether auditor must review DPDP legal compliance (consent flows) or focus only on technical controls.	Requirements are specified in RFP. Please comply with the RFP T&C's.
78	Cloud Assurance Reports	25	Cloud SOC2 Type II, user-entirey controls.	Confirm whether CFHL will provide CSP SOC2 Type II reports or if alternate certifications (ISO 27001/CSA STAR) are acceptable where SOC2 is unavailable.	Successful bidder will be given additional information about the CBS implementation.
79	Pre-bid Meeting Date & Time	2	Pre-bid Meeting Date & Time	We request you to kindly allow us to participant the pre-bid meeting online.	Link will be shared.
80	8. Evaluation Criterion:	8	1. (A) Experience in conducting Infrastructure, Application, and Security Audits of Core Business Solutions (CBS) or similar large-scale IT systems in Banking/Financial Institutions/NBFCs/Housing Finance Companies or other Critical Infrastructure Institutions: • More than 3 years - 15 marks • >2 years and ≤3 years - 10 marks • ≥1 year and ≤2 years - 05 marks • Less than 1 year - 0 marks	•Please confirm number of work order to be submitted and for which year. •We understand that if we have conducted security audits for two separate years for the same organization under a single agreement/PO, the same will be counted as two separate instances. Please confirm. •We assume work order from NHB/SEBI (regulators) will be considered. •We understand that if we are conducting security audit for 2 separate years for same organization under a single agreement / PO , the same will counted as 2 instances. Kindly confirm Please confirm the number of work orders required to be submitted and the applicable year(s). •We assume that work orders issued by regulators such as NHB / SEBI will be considered. Kindly confirm.	Each PO or relevant acceptable documents will be considered for evaluation with the evaluation committee subjected to T&C's of the RFP. The same was clarified in pre-bid meeting.
81	8. Evaluation Criterion:	8	1. (B) Past Experience of conducting Infrastructure, Application, and Security Audits of CBS or similar large-scale IT systems in BFSI sector organizations / NBFCs / Scheduled Commercial Banks / Government Departments / PSU organizations / Housing Finance Companies in India. 3 projects in the last 2 years (5 marks each)	•Please confirm the number of work orders required to be submitted and the applicable year(s). •We assume that work orders issued by regulators such as NHB / SEBI will be considered. Kindly confirm. •We understand that if we have conducted security audits for two separate years for the same organization under a single agreement/PO, the same will be counted as two separate instances. Please confirm.	Each PO or relevant acceptable documents will be considered for evaluation with the evaluation committee subjected to T&C's of the RFP.
82	8. Evaluation Criterion:	8	2. (C) Bidder presentation	We request you to kindly allow us to participant the presentation online.	This will be discussed after evaluation of Part A as per the T&C's of the RFP and directions from evaluation committee.
83	42. ANNEXURE-VI: Scope of Work:	22-40	ANNEXURE - VI: Scope of Work: a) Scope of work:	<u>Process Audit:</u> 1) As per our understanding the scope mentioned in the section (d) Detailed scope of work, related to only the CBS Application and not any other application. Kindly confirm. 2) What would be the location of the audit? 3) Whether the revalidation/compliance audit would be part of audit scope. 4) What is the location of the DC and DR. 5) Whether the data migration audit would be part of audit scope. Kindly confirm. If yes, kindly share the details of the pre and post migration data (Table Count and Table Size). 6) Whether the audit need to be carried out post implementation of entire module or as an when it is developed. Kindly confirm total number of audit cycle. 7) Whether the application/database is hosted on the cloud environment. <u>Technical Audit:</u> 1) Total Nos. Network Architecture Review/ Location. 2) Web application Audit (Total Number of websites to be covered No. of static pages No. of Dynamic pages, No. of input fields, Types of user, Roles of each user). 3) Mobile application Audit - Total Number of Applications to be covered ,No. of Screens ,No. of input fields ,Nos(Android, iOS, Windows) for each application ,Black box or grey box testing 4) Application Source Code Audit to be covered (Line of code required for each application). 5) Total Nos. Web service to be covered (Methods required for each application). 6) Locations of Audit Required for each activity along with its inventory details. 7) DC/DR/ NDR Location required. 8) No. of Servers (including type of operating system and Database). 9) No. of Desktop/Laptop and their location. 10) No. of Firewall. 11) No. of IDS / IPS. 12) No. of Routers. 13) No. of Switches. 14) Whether configuration audit is required. If yes, provide counts for Network Devices, Security Devices, OS, and Databases. 15) No of external IP addresses. 16) Is it a one-time Comprehensive Audit, or will it also include compliance audit, revalidation, and retesting activities. 17) Whether an Information Systems Audit has been performed earlier. If yes, provide auditor name, scope of work, and audit year. 18) Is department using NMS Tools? 19) Any additional activities that must be covered but are not mentioned above then please specify.	1) Refer Annexure VI of the RFP. 2) In person audit. Location is in Head Office Bangalore. 3) Yes 4) On AWS Cloud 5) Kindly refer Annexure VI of the RFP 6) Audit needs to be carried out on phase wise applications roll outs. 7) Yes 1-19) This will be shared with the successful bidder.
84	Pre-Contract Integrity Pact	45	Pre-Contract Integrity Pact (This has to be submitted in the non-judicial Stamp Paper of requisite value in Bangalore, Karnataka)	• Kindly clarify whether the Integrity Pact is required to be submitted at the time of bidding or after the bidder is declared L1. • Please confirm whether the Integrity Pact needs to be submitted on stamp paper. If yes, kindly specify the value of the stamp paper required.	As per the integrity pact below clause is mentioned WHEREAS THE BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER has clearly understood that the signing of this agreement is an essential pre-requisite for participation in the bidding process in respect of Stores/Equipment/Items/Services proposed to be procured by the BUYER and also understood that this agreement would be effective from the stage of invitation of bids till the complete execution of the agreement and beyond as provided in clause 13 and the breach of this agreement detected or found at any stage of the procurement process shall result into rejection of the bid and cancellation of contract rendering BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER liable for damages and replacement costs incurred by the BUYER. Needs to be submitted in stamp paper of Rs 500.

85	EARNEST MONEY	47	5.1. Every BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER while submitting commercial bid, shall deposit an amount as specified in RFP/Tender Documents as Earnest Money, with the BUYER through any of the instruments as detailed in the tender documents.	- After reviewing the RFP, we noticed that the EMD and tender fee amounts are not mentioned. Kindly confirm whether we are required to submit the EMD. - As we are an MSME-registered company, we request you to consider the exemption provided under the MSME Act, wherein MSEs are exempted from payment of EMD and tender fees. Accordingly, we request you to kindly waive the EMD/tender fee for MSMEs.	EMD, Tender fee are not required for this engagement.
86	APPENDIX-A-Part A	50	Part A- Conformity to Eligibility Criteria 2) Power of Attorney/Authorization letter signed by the Competent Authority with the seal of the bidder's company/firm in the name of the person signing the tender documents.	As we understand that we do not have to submit the power of attorney . As a board resolution has already been passed for general power of attorney and can be signed by the Director. As a result, we will submit the board resolution instead of the Power of Attorney. Please confirm.	Valid Board Resolution authorizing the signatory will also be accepted in lieu of the Power of Attorney.
87	Confidentiality and Non-Disclosure Agreement	55	Confidentiality and Non-Disclosure Agreement	- Kindly clarify whether the NDA is required to be submitted at the time of bidding or after the Bidder is declared L1. - Please confirm whether the Integrity Pact needs to be submitted on stamp paper. If yes, kindly specify the value of the stamp paper required.	NDA will be signed with the successful bidder. Integrity Pact needs to be submitted in stamp paper of Rs 500 of the relevant state. This was clarified in Pre-bid meeting.
88	Annexure		Annexure	Can you provide the Annexure in word document?	The documents will be given in PDF format only.
89	46. ANNEXURE – X – Bill of Material	44	Generic Audit	What activities does the audit agency need to cover under generic audit. Is there any particular circular against which audit is to be performed.	Audit has to be completed as per the scope of the RFP and there are no audit circulars.
90	46. ANNEXURE – X – Bill of Material	44	Delivery Audit	What activities does the audit agency need to cover under delivery audit. Is there any particular circular against which audit is to be performed.	Audit has to be completed as per the scope of the RFP and there are no audit circulars.
91	EXHIBIT A	27	Security Audit Related	Kindly share no. of applications for which source code review to be conducted. Kindly share counts of web application, mobile application and APIs. Kindly share no. of thick client applications.	Successful bidder will be given additional information about the CBS implementation.
92	EXHIBIT A	27	Security Audit Related	Kindly share Network Infrastructure details such as no. of servers, routers, switches etc. for which VAPT is to be performed and also the frequency of audit.	Successful bidder will be given additional information about the CBS implementation.

** RFP-IT/140/2024-26 can be accessed at the following link:
<https://www.canfinhomes.com/Tenders/archivetender>