CANARA ROBECO

Asset Management Company Limited

REQUEST FOR PROPOSAL

FOR

Procurement of Cloud & HCI Services for hosting Servers

This request for proposal for selection of the Cloud Service and HCI Service provider for the proposed IT Infrastructure is issued for private purposes only and is not a public document and issued _____ for bidding for the _____. This document is meant for the exclusive purpose of Bidding as per the Specification Terms, Conditions and Scope indicated and shall not be transferred, reproduced, or otherwise used for purposes other than for which is specifically issued.

Important Note: Applications in response to this RFP are invited to carry out a preliminary evaluation to assess the suitability of the Bidders to take up the assignment based on our internal norms and accordingly, to shortlist the bidding firms not exceeding five for the purpose of moving to the second phase of technical and commercial bidding process.

Index

1. ABOUT THE COMPANY

Canara Bank, a government-owned institution with over 118 years of experience, serves over 89 million customers through 9,816 branches across India. Rated AAA by CRISIL, it stands as one of India's oldest and largest banks.

OCE is a 100% owned subsidiary of ORIX Corporation, Tokyo ("ORIX Corporation") a Japanese conglomerate listed on the Tokyo Stock Exchange and New York Stock Exchange and operating in financing and investment, insurance, banking, asset management, real estate, public works, environment and energy, civil engineering and transport. ORIX Corporation acquired Robeco Groep N.V. in two steps in 2013 and 2016, and Robeco Groep N.V. changed its name to ORIX Corporation Europe N.V. on January 1, 2018.

Canara Bank, with over a century of experience, and Robeco, offering global investment expertise, combine to bring collective knowledge. Together, they deliver strong, sustained performance to secure your financial future.

2. ELIGIBILITY CRITERIA

Vendor will be eligible if he complies with Annexure I for Cloud Service provider and Annexture II for HCI service provider.

3. SCOPE OF WORK

The selected firm will have to stick to the following Scope of Work (Cloud) :

- Implementation of an end-to-end installation of Cloud solution with required Hardware and software.
- Data localization criteria should be met.
- Cloud services provider (CSP) should be MeitY empaneled and the Data Centers including DR should be based in India.
- Data at rest, transit, and replication to any data Centre outside the boundaries of the country (India) is not allowed.
- Data should be stored at REST with 256-bit encryption with integrated KMS for key management
- System must be resilient with VM protection
- Complete solution should provide dedicated Perimeter security and endpoint XDR with complete visibility dashboard for CRAMC.
- Need to provide Integrated NOC/SOC platform
- Cloud providers should consider dedicated required load balancers for application access with throughput of 3 Gbps Minimum.
- Cloud provide should consider backup solution for protection VM and Database Data along with 2-1 Framework (1 Copy will be at cloud provider DC, Second will be at DR)
- Cloud providers should consider backup server / software components along with storage for DC and DR.
-

- Backup data must be stored with minimum 256-bit encryption with retention period is daily incremental - 6, weekly full - 4, Monthly full - 12 and yearly - 10
- The Vendor is required to provide training to the Company's Technology team on the proposed RFP Solution, provide a training schedule and furnish training details as per the RFP requirements.
- Bidders should conduct proper knowledge transfer as per CRAMC's requirement.
- The bidder shall be responsible for provisioning of required IAAS, PAAS or SAAS, depending on the management decisions CRAMC would like the Bidder to design and deploy a landing zone along with the cloud foundation setup (Creating the Organization Resource and Billing Account) for their organization.
- The proposed solution should offer the ability to create a data platform to support business insights and machine learning.
- The solution should offer scalability to support the CRAMC's volumes and growth – covering elasticity, auto scaling and serverless operations. The solution should provide CRAMC with the ability for the data platform to scale elastically as data storage and compute requirements grow + effectively handle situations where multiple workloads compete for the same set of limited resources.
- The solution design must offer at least 99.9% uptime per calendar month as a formal SLA.
- The solution must offer a platform to mask or encrypt data based on CRAMC requirements.

The selected firm will have to stick to the following Scope of Work (Hyper-Converged infrastructure) :

- Implementation of an end-to-end installation of Hybrid Cloud solution with required Hardware and software.
- Data localization criteria should be met.
- Hardware and Encryption should be Post-Quantum Cryptography Compliant.
- The Vendor is required to provide training to the Company's Technology team on the proposed RFP Solution, provide a training schedule and furnish training details as per the RFP requirements.
- Bidders should conduct proper knowledge transfer as per CRAMC's requirement.
- The bidder shall be responsible for provisioning the required HCI in a hybrid mode. Depending on the management decisions CRAMC would like Bidder to design and deploy microsegmentation.
- The proposed solution should offer the ability to create a data platform to support business insights and machine learning along with Dashboard.
- Management console of the Platform must be Active-Active Highly available which will provide end to end complete management in non-disruption mode , Bidder has to consider all required license of additional component for Management high availability which include OS license as well CRAMC will not provide any additional license of windows OS for the same.
- Bidder should Proposed platform with solution and replication tool which will integrate with CRAMC Existing cloud and provide between 15min to 30min Replication RPO for VM.
- Bidder has to provide solution of HCI along with required 10 Gbps Ethernet switches in High availability along with uplink to On premise network.
- The solution should offer scalability to support the CRAMC's volumes and growth – covering elasticity, auto scaling and serverless operations. The solution should provide CRAMC with the ability for the data platform to scale elastically as data storage and compute requirements grow + effectively handle situations where multiple workloads compete for the same set of limited resources.

- The solution design must offer at least 99.99% uptime per calendar month as a formal SLA.
- The solution must offer a platform to mask or encrypt data based on CRAMC requirements.

Data migration

- Bidder should develop a data migration strategy covering data migration and testing, in consultation with CRAMC.
- Bidder is expected to ensure best practices while migrating data to cloud and implement different security services available as part of the solution subscribed by the CRAMC.

Monitoring & Alerting

- Cloud native services-based monitoring & alerting
- HCI native Services need to be enabled for monitoring

Technical Support Services

- Issue/Request logging, updates,
- Troubleshooting & Resolution/Request fulfilment

Management Services

- Environment deployment as designed,
- Process and implement environment change requests,
- Resource/Capacity changes,
- Virtual network setup, changes,
- Environment access setup, changes

Backup & Restore

- Setup and maintain snapshots,
- Maintain backups, monitor backup jobs.

Advanced Services

- Support/Participate for DR tests (Once in a Year),
- Cost optimization services,

Considering the extensive nature of the assignment and the envisaged relationship with the Bidder, any service, which forms a part of facilities management that is not explicitly mentioned in this RFP as excluded would form part of this RFP, and the Bidder is expected to provide the same at no additional costs to the Company. The Bidder must envisage all necessary services to be provided and ensure the same is delivered to the Company. The Company will not accept any plea from the Bidder at a later date for omission of critical services on the pretext that the same was not explicitly mentioned in the RFP.

The Bidder will be required to fix any vulnerability in the RFP for Selection of partner to provide Cloud /HCI Solution at no additional cost during the entire tenure of the contract. These vulnerabilities can be detected by CRAMC or can be a finding of any internal or external audit conducted by the CRAMC or its auditors on a periodic basis.

Supply and licensing.

The Cloud Service Provider ("CSP") shall provide CRAMC with licenses for the operating system(s) for the duration of the Agreement term. These licenses entitle CRAMC to install and use the operating system(s) on the virtual machines or servers provisioned by the CSP.
CRAMC will not be responsible or liable for any infringements or unauthorized use of the licensed products by the Bidder in performance of any activity/obligations undertaken by the Bidder in terms of this RFP. In the event of any claims against CRAMC for any license related issues, the selected Bidder will have to act upon the same and all liabilities and claims whatsoever will have to be settled by the selected Bidder and the CRAMC shall be kept indemnified against any such liabilities.

The HCI Service provider shall provide CRAMC with Windows Server Licenses bundle with HCI solution or mention in separate line item. Further if the selected Bidder has missed out providing any required licenses to CRAMC, then CRAMC will not bear any additional amount for procurement of such licenses later.

The CSP shall provide updates and patches for the operating system(s) and database software(s) during the term of the Agreement, as applicable.

Onsite support services:
The Bidder shall depute dedicated supported on need base, at the CRAMC Headquarters.

Qualification & Experience of Personnel for Support:
The product installation and maintenance shall be done by trained & experienced personnel, having current knowledge on the solution, operating systems, networking, firewall, IPS, information security awareness.

CRAMC reserves the right to ask for replacement of the engineers based on their performance. Bidder must replace such engineers with competent resource complying with the qualification and experience mentioned in the RFP within 15 days from the date of communication from the CRAMC.

Description	Minimum Qualification
L3	Should have minimum degree in Computer Science/ IT/ similar technology related stream or equivalent with minimum 7 years of relevant post qualification experience in similar solutions as proposed in this RFP. L3 resource will be responsible for end-to-end management of the solution including installation, configuration, troubleshooting, managing onsite resources, coordinating with OEM etc.
L2	Should have minimum degree in Computer Science/ IT/ similar technology related stream or equivalent with minimum 4 years of relevant post qualification experience in similar solutions as proposed in this RFP. L2 resource should coordinate with L1 & L3 resources for smooth functioning of the project 24x7x365.
L1	Should have minimum degree in Computer Science/ IT/ similar technology related stream or equivalent with minimum 1 year of relevant post qualification experience in similar solutions as proposed in this RFP.

4. SUBMISSION OF PROPOSAL

Proposals are required to be submitted as per the following directions and as per the formats mentioned in Annexures.

"Application for SELECTION OF CLOUD SERVICES."

4.1. Envelope 1 (unsealed) containing the following:

i) Refundable fee of Rs Fifty Thousand by way of a demand draft drawn in favor of Canara Robeco Asset Management Company Limited payable at Mumbai
ii) A letter authorizing the person to sign the proposal and other documents on behalf of the Bidder,
iii) Certificate/Declaration (if any).

4.2. Envelope 2 (sealed) containing the Technical Bid as per Proposal Format - Annexure IV.

4.3. Envelope 3 (sealed) contains the Financial Bid, to be opened by CRAMC. privately, after the technical evaluation. The bids will not be opened in presence of the shortlisted Bidders.

4.4. The proposed procurement/ subscription would be for 5 years (i.e. from Month, Date, 2026, to Month Date, 2029) and shall be renewed for a further period subject to review by CRAMC.

4.5. The Company reserves the sole right to shortlist and award the assignments based on specified. criteria and subject to approval of the appointment by Competent Authority.

4.6. Mere submission of application does not, in any way, constitute a guarantee for award of any. assignment by the Company

Please note that the financial bid shall be considered valid for 90 days from the date of submission of the bid.

The proposal (all three envelopes) can be submitted at the latest by 17:00 hours on 8th January 2026, at CRAMC office, at **Construction House, 4th Floor, 5, Walchand Hirachand Marg, Ballard Estate, Mumbai 400 001** in hard copies in original, duly signed by the authorized officer of the Bidder. The sealed Bid envelopes should be delivered to the CRAMC Office between 10:00 hours to 17:00 hours on Monday to Friday, working days only.

For any queries, please contact Mr. Vivek Mhatre, Sr. Manager, Email id: cramc.it@canararobeco.com.

No proposal will be entertained after the appointed time and date. The Company will not be responsible for any postal/ courier delay. The proposals received after the appointed time and date will be rejected.

Proposals with any conditionality shall be summarily rejected. Financial aspects of the proposal should

not be disclosed in any way other than in the financial bid. Technical bids containing any indication to the financial bids will be rejected.

Incomplete proposals, conditional proposals, proposals not conforming to the terms and conditions set out herein will be rejected by the Company.

Misrepresentation of any fact within the proposal would lead to cancellation of the contract apart from any other actions which the Company would be entitled to take.

The Company reserves the sole right to accept or reject any or all Proposals received without assigning any reasons thereof. The decision of the Company / Committee on the selection of the bidder shall be final.

5. TIME FRAME

The following is an indicative time frame for the overall selection process. The Company reserves the right to revise/modify this time frame at its absolute and sole discretion and without providing any notice/intimation or reasons thereof to any of the Bidders. Changes to the time frame will be conveyed to the affected Bidders during the process.

RFP Notification	
Last date of submitting queries	30th December 2025
Last Date of Proposal Submission	9th January 2026
Opening of Technical Bid	13th January 2026
Opening of Commercial Bid	16th January 2026

6. PROCEDURE FOR SELECTION

6.1 Qualified interested Bidders, need to meet the set criteria and comply with all compliance checklists.

6.2 The Committee would evaluate the bidders on the criteria mentioned in Proposal Format based as per Annexure IV and proposals received and shortlist bidders scoring above a pre-determined threshold or any other criteria that Committee may deem fit.

6.3 The Committee will open the Financial Bids of shortlisted bidders as per internal procedure. The date and time of opening of the Financial Bids will be announced as per RFP Notification.

6.4 The marks scored by shortlisted bidders in the technical evaluation will then be given a weightage of seventy percent. Similarly, the Financial Bids of the bidders will be given a weightage of thirty percent. The combined score of Technical and Financial Bids will determine the H1 (Bidder scoring highest point / marks), H2, H3 and so on. The Company will select such number of bidders as deemed appropriate who agree to undertake the assignment. The Company will use waterfall

for the next bidder in case any shortlisted bidder does not accept the appointment. The Bid scores will not be made public, and neither will the Bids be opened in the presence of the Bidders.

6.5 The bidder scoring the highest points/marks (H1) based on the above principles would be appointed for the transaction. Other Bidders will be updating their status accordingly.

7. REQUIREMENTS OF FINANCIAL BID

7.1 The fee quoted should be unconditional. Each bidder is required to submit its financial bid along with a covering letter and financial bid in the format prescribed in Annexure V.

7.2 The fee quoted by the Bidder should be exclusive of Goods and Services Tax but inclusive of out-of-pocket expenses etc. The Goods and Services Taxes should be indicated separately while raising the bills for payment of fee. All bills are to be raised in INR and will be payable in INR only after successful and satisfactory closure of the transaction.

7.3 Invoices to be generated in Financial Year 2026-2027.

8. COMPLIANCE

8.1 Due Diligence

The Bidder is expected to examine all instructions, forms, terms, and specifications in this RFP. Application shall be deemed to have been done after careful study and examination of this RFP with full understanding of its implications. The Application should be precise, complete and in the prescribed format as per the requirement of this RFP. Failure to furnish all information required by this RFP or submission of Application not responsive to this RFP in every respect will be at the Bidder's risk and may result in rejection of the Application.

Confidentiality

The Invitation document is confidential and is not to be disclosed, reproduced, transmitted, or made available by the Recipient to any other person. The Invitation document is provided to the Recipient on the basis of undertaking of confidentiality given by the Recipient to Company. The company may update or revise the document or any part of it. The Recipient acknowledges that any such revised or amended document shall be received subject to the same confidentiality undertaking. The Recipient will not disclose or discuss the contents of the document with any officer, employee, consultant, director, agent, or other person associated with or affiliated in anyway with Company or any of its customers or suppliers without the prior written consent of Company.

8.2 Cost of Participation

The Bidder shall bear all costs associated with the preparation and submission of its Application and CRAMC, will in no case be held responsible or liable for these costs, regardless of the conduct or outcome of the selection process.

8.3 Clarification of RFP Documents

A prospective Bidder requiring any clarification on this RFP may contact CRAMC in writing by E-mail at cramc.it@canararobeco.com. CRAMC shall respond in writing by E-Mail to any request for clarification of the application documents, from the prospective Bidders, which it receives not later than 8th January 2026. Further CRAMC will respond by E-Mail to all clarifications, without identifying the source of the inquiry. CRAMC shall not be responsible for any external agency delays.

8.4 Amendment of RFP Document

a) CRAMC reserves the sole right to include any addendum to this entire selection process. The Bidders shall not claim as a right for requiring CRAMC to do the previously mentioned.

b) At any time before the deadline for submission of proposals, CRAMC may, for any reason, whether at its own initiative or in response to a clarification requested by prospective Bidders, modify this RFP Document.

c) All Bidders who have responded to this RFP shall be notified of the amendment in writing by e-mail, fax, or post, and all such amendments shall be binding on them.

d) If required, in order to allow prospective Bidders reasonable time in which to take the amendment into account in preparing their applications, CRAMC reserves the right to extend the deadline for the submission of applications. However, no request from the Bidder shall be binding on CRAMC for the same.

9. INFORMATION REQUIRED

9.1. Mandatory information to be submitted on the letter head of the firm to be eligible for the bidding process (Please attach as Annexure I):

Sr.No.	Item	Details
Basic Data		
1.	Name of the Firm	
2.	Address of Head Office Number of Branch Offices (Specially mention the office address, Partner and other details of the contact person in Mumbai office)	
3.	Constitution	
4.	Date of Establishment	
5.	Registered Office Address	
6.	GST Number	
7.	Whether the Firm or any partner has ever been debarred by	

	RBI/SEBI if yes, details: Registration Number Name of the partner Brief reasons for debarment Note: Firm includes Partnership Firm, LLP, or a limited Company. Partners include director as well.	
8.	Name, Designation, Tel. No, E-Mail of the authorized signatory submitting the RFP (Please enclose the copy of board resolution)	
9.	Any pending or past litigation (within three years)? If yes, please give details	
10.	Turnover for the past 3 years (FY, Turnover, Net Profit, Net Worth)	
12.	Brief profile of Partners/Director in the following manner)	

Name/ Qualification	Total Experience	Experience with Current firm	Project Details

12. Past Experience of similar nature

Name NBFC/ AMC	Nature Of Assignment	Year of Assignment	Project Manager	No of Applications

10. DOUCMENTS TO BE SUBMITTED

Bidder shall submit the following documents along with the application.

i) Mandatory information as per point No. 2.1 above

ii) Copies of certificate of experience including project details etc., in relation to similar assignment performed elsewhere, if any.

iii) Copies of Registration Certificate issued to the firm.
iv) Copy of constitution Certificate issued.
v) STQC or similar Compliance of the product (If any)
vi) Use case of Cloud migration for same kind of setup.
vii) Acceptance Letter of the RFP and its provisions
viii) Project Plan and Approach
ix) Presentation of the Proposed Solution (The bidder may be required to present solution if requested by CRAMC Team)
x) Any form of canvassing/lobbying/influence/cartelization, etc. by the Bidder may result in disqualification of such Bidder.
xi) Letter of confirmation regarding non-disqualification as per Annexure - III

11. GENERAL CONDITIONS

i.	No communication will be sent by CRAMC, and no correspondence will be entertained with respect of firms, which are not being selected.
ii.	The selected Firm, on receiving the offer letter from CRAMC, shall submit hard copies of Letter of acceptance of terms and conditions, undertaking letter, and Undertaking of Fidelity and Secrecy (Formats will be shared with the selected firm).
iii.	The assignment should be conducted in a professional manner and in case of any misconduct & negligence, CRAMC is free to report the matter to SEBI/RBI under the guidelines from time to time. This will be in addition to the disengagement from the assignment.
iv.	By virtue of the engagement, the successful Bidder's team may have access to business information of CRAMC. CRAMC shall at all times have the sole ownership of and the right to use all such data in perpetuity in the course of performing the Service(s) under the Engagement.
v.	Appointment of Firms shall be purely at the discretion of CRAMC, and no rights whatsoever accrue to the firm for such appointment.
vi.	**Regulatory Compliance:** Cloud service provider shall strictly comply with all the requirements laid down in SEBI circular No. SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/ 033, dated March 06, 2023, and any non-compliance of the conditions specified in the said circular will be subject to rejection.
vii.	CSP shall adhere to the coverage strictly as per the scope as may be decided by CRAMC from time to time.
viii.	CRAMC reserves the right to seek views from the entities with whom the firm is/has been/was associated.
ix	The firm shall not sub-contract or assign part of the scope of work to any outside firm or other person without express permission in writing from CRAMC.
X	In case of HCI, Hardware to be delivered in March 2026 for deployment. Invoice will be generated in financial year 2026-27.
XI	Any other terms and conditions of the assignment would be decided by CRAMC on a case-to-case basis.

12. PLANNING & EXECUTION:

I. Implementation Methodology -

a. The selected Bidder should follow a suitable methodology for delivering the requirements of the RFP for the entire contract period. Accordingly, the Bidder should factor for necessary effort and team deployment. The methodology should clearly lay out the overall steps from initiation to closure of this engagement.

b. The FRSM (Functional Requirements Specification Manual) would be reviewed by the Company, and the selected bidder is expected to remediate all gaps identified by the Company.

II. Functional Requirements specifications Manual (FRSM)

a. The selected bidder will conduct a detailed systems requirements study and provide a solution specific FRSM for solutions relating to the functionalities as required supporting various processes within the Company as responded by the Bidder.

b. The FRSM should include the standard operating procedure proposed for the re-aligned process. Bidder is expected to assist the Company in aligning the business requirements with the application so as to enable centralization of desired business process, eliminate redundant and duplicate processes, increase operational efficiency, and improve customer service.

c. The bidder is expected to prepare detailed documentation, presentation, workflows for the business processes affected due to implementation of the RFP for Selection of partner.

d. The Bidder shall provide the FRSM to the Company for review and comments and any comments or suggestions of the Company will be incorporated therein.

e. The Company will identify spocs for each process, which would be responsible for the review, comments, and sign–off of the FRSM (FRSM – Please refer to Annexure IV)

f. The FRSM will be deemed completed when signed off from the Company.

III. Business Process Definition (BPD)/Parameterization

a. The selected bidder is also expected to conduct and document a detailed current assessment of all business activities and services performed by the Company to gain understanding of the Company's existing business and operations.

b. The selected bidder is expected to help the Company to parameterize the product and provide valuable input at the time of system parameterization based on the current state assessment undertaken by the selected bidder. Also, the core team training conducted by the selected bidder should reflect an understanding of the Company's current processes because of conducting the current assessment.

c. The selected bidder would be responsible for ensuring that the BPD/Parameterization exercise is as per the plan.

13. TENURE OF ASSIGNMENT

CRAMC in the first instance will appoint the shortlisted CSP for three (3) financial years. The term may be extended solely at the discretion of CRAMC on satisfactory review by the competent authority.

14. CONDUNT & PERFORMANCE MONITORING

a. CRAMC shall designate one of its senior officers as a single point contact for coordinating the assignment.

b. CRAMC shall provide the requisite initial information of its activities and further support.

c. CRAMC reserves the right to review the appointment at any point of time and if necessary, to cancel the appointment by giving 7 days' written notice. In the event of termination of contract, a further course of action which might include transition would be decided as per the agreed terms and conditions.

d. In case the firm fails to report serious omissions/ commissions/ non-compliance etc., CRAMC reserves the right to report the matter to SEBI/ RBI, which may result in appropriate action. Such firms will not be eligible for any further service contract with CRAMC for the next five years.

15. REPRESENTATIONS & WARRANTIES:

a. That the Bidder is a Partnership firm/LLP/Company with requisite qualifications, skills, experience, and expertise in providing Service(s) contemplated herein, the financial wherewithal, the power, and the authority to enter into the Engagement and provide the Service(s) sought by CRAMC.

b. That the Bidder is not involved in any major litigation, potential, threatened and existing, that may have an impact of affecting or compromising the performance and delivery of Service(s) under this Engagement.

c. That the representations made by the Bidder in its application are and shall continue to remain true and fulfill all the requirements as are necessary for executing the duties, obligations and responsibilities as laid down in the Engagement and the RFP Documents and unless CRAMC specifies to the contrary, the Bidder shall be bound by all the terms of the RFP.

d. That the Bidder has the professional skills, personnel and resources/authorizations that are necessary for providing all such services as are necessary to perform its obligations under the application and this Engagement.

e. That the Bidder shall use such assets of CRAMC as CRAMC may permit for the sole purpose of execution of its obligations under the terms of the RFP or the Engagement. The Bidder shall however, have no claim to any right, title, lien, or other interest in any such property, and any possession of property for any duration whatsoever shall not create any right in equity or otherwise, merely by fact of such use or possession during or after the term hereof.

a. That the Bidder shall procure all the necessary permissions and adequate approvals and licenses for use of various software and any copyrighted process/products free from all claims, titles, interests, and lien thereon and shall keep CRAMC, its directors, officers, employees, representatives, consultants and agents indemnified in relation thereto.

b. That all the representations and services as have been made by the Bidder with respect to its RFP and Engagement are true and correct and shall continue to remain true and correct throughout the term of the Engagement.

c. That the execution of the Service(s) herein is and shall be in accordance with and in compliance with all applicable laws.

d. That there are – (a) no legal proceedings pending or threatened against Bidder or any of its partners or its team which adversely affect/may affect performance under this Engagement; and (b) no inquiries or investigations have been threatened, commenced, or pending against the Bidder or any of its Partners or its team members by any statutory or regulatory or investigative agencies.

e. That the Bidder has the corporate power to execute, deliver and perform the terms and provisions of the Engagement and has taken all necessary corporate action to authorize the execution, delivery, and performance by it of the Engagement.

f. That all conditions precedent under the Engagement have been complied with.

g. That neither the execution and delivery by the Bidder of the Engagement nor the Bidder's compliance with or performance of the terms and provisions of the Engagement (i) will contravene any provision of any applicable law or any order, Regulation, writ, injunction or decree of any court or governmental authority binding on the Bidder (ii) will conflict or be inconsistent with or result in any breach of any or the terms, covenants, conditions or provisions of, or constitute a default under any agreement, contract or instrument to which the Bidder is a party or by which it or any of its property or assets is bound or to which it may be subject.

16. CONFIDENTIALITY

The Parties agree that they shall hold in trust any Confidential Information received by either Party, under the Engagement, and the strictest of confidence shall be maintained in respect of such Confidential Information. The Parties agree to execute the Confidentiality Agreement prior to finalization of Engagement and shall abide by the terms and conditions of confidentiality as contained therein.

17. GOVERNING LAW

The Engagement shall be governed in accordance with the laws of Republic of India. These provisions shall survive the Engagement.

18. JURISDICATION OF COURTS

The courts of India at Mumbai shall have exclusive jurisdiction to determine any proceeding in relation to the Engagement. These provisions shall survive the Engagement.

19. TIME LIMIT FOR COMMENCEMENT OF WORK

Time limit for commencement of work shall be mutually decided at the time of award of Engagement.

Bidders need to complete the attached annexures:

1. Compliance Requirements (on the letter head of the firm) – Annexure - I
2. Application format for Procurement of Cloud services / Hyper Converged Infrastructure (on the letter head of the firm) – Annexure - II
3. Letter of confirmation regarding non-disqualification (to be submitted on letter head) – Annexure - III
4. FRSM Specification – Annexure – IV – Sheet attached with Tender notice.

5. Commercial bid format - Annexure – V

20. DISCLAIMERS

The information contained in this RFP document or information provided subsequently to Bidders whether verbally or in documentary form by or on behalf of Canara Robeco Asset Management Company Limited (CRAMC), is provided to the Bidder(s) on the terms and conditions set out in this RFP document and all other terms and conditions subject to which such information is provided.

This RFP document is not an agreement and is not an offer or invitation by CRAMC to any parties other than the Bidders who are qualified to submit the applications as per the eligibility conditions. The purpose of this RFP is to provide the Bidder(s) with information to assist in the formulation of their proposals. This RFP does not claim to contain all the information each Bidder may require. Each Bidder firm should conduct its own investigations and analysis and should check the accuracy, reliability, and completeness of the information in this RFP. CRAMC makes no representation or warranty and shall incur no liability under any law, statute, rules, or regulations as to the accuracy, reliability or completeness of this RFP.

The information contained in the RFP document is selective and is subject to updating, expansion, revision and amendment. It does not purport to contain all the information that a Bidder may require. CRAMC does not undertake to provide any Bidder with access to any additional information or to update the information in the RFP document or to correct any inaccuracies therein, which may become apparent. CRAMC reserves the right or discretion to change, modify, add or alter any or all of the provisions of this RFP document and / or the selection process, without assigning any reasons, whatsoever. Such change will be intimated to all Bidders. Any information contained in this RFP document will be superseded by any later written information on the same subject made available to all recipients by CRAMC.

CRAMC may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP.

CRAMC reserves the right to reject any or all expressions of interest / proposals received in response to this RFP document at any stage without assigning any reason whatsoever. The decision of CRAMC shall be final, conclusive, and binding on all the parties.

12.1 No legal relationship

No binding legal relationship will exist between any of the Bidders and the CRAMC until execution of a contractual agreement with the successful Bidder.

12.2 Evaluation of Offer

Each Bidder acknowledges and accepts that the Company may, in its absolute discretion, apply any additional criteria it deems appropriate in the selection of the bidder, not limited to those selection criteria set out in this RFP.

12.3 Disqualification

Any form of canvassing/lobbying/exercise of influence/cartelization etc. by the Bidder will result in disqualification of such Bidder.

In case it is found during the course of the transaction or at any time before award of the assignment or after its execution and during the period of subsistence or after the period thereof, that one or more of the terms and conditions laid down in this Request for Proposal has not been met by the Bidder, or the Bidder has made material misrepresentation or has given any materially incorrect or false information, the Bidder shall be disqualified forthwith if not yet appointed as the CSP (Customer Support Partner). Also, if the Selected Bidder has already been appointed as the CSP, as the case may be, the same shall, notwithstanding anything to the contrary contained in this RFP, be liable to be terminated, by a communication in writing by the CRAMC to the Selected Bidder without the CRAMC being liable in any manner whatsoever to the CSP. This action will be without prejudice to any other right or remedy that may be available to the CRAMC under the bidding documents, or otherwise. However, before terminating the assignment, a show cause notice stating why its appointment should not be terminated would be issued giving it an opportunity to explain its position.

12.4 Confidentiality

The information contained in this document is confidential. The Bidder shall not share this information with any other party not connected with responding to this RFP. The information contained in this RFP or subsequently provided to Bidder(s) whether verbally or in writing by or on behalf of the CRAMC shall be subject to the terms and conditions set out in this RFP and any other agreement/contract to be executed by the CRAMC.

12.5 No representation or warranty by the CRAMC

The CRAMC makes no representation or warranty and shall incur no liability under any law, statute, rules, or regulations on any claim the potential bidder may make in case of failure to understand the terms and requirements of this RFP and responds to the RFP.

The CRAMC may, in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP and specify additional requirements or cancel this RFP at any time without assigning any reason there of and without any notice, at its sole discretion. All such changes or events will be uploaded on CRAMC's website at www.canararobeco.com. Interested parties are advised to regularly refer to the URL mentioned above.

While due care has been taken in the preparation of this document, the CRAMC will not be held responsible for any inaccuracy in the information provided herein. The Bidder must apply its own care and conduct its own investigation and analysis regarding any information contained in the RFP document and the meaning and impact of all such information contained in the RFP.

It is the Bidder's responsibility to examine this RFP; examine all other information available on reasonable inquiry relevant to the risks, contingencies and circumstances affecting its response to the RFP; and satisfy itself as to the completeness, correctness, and sufficiency of all the information contained in its response to the RFP.

12.6 CRAMC's Discretion

i) The CRAMC may at its sole discretion select and appoint such number of bidders as it deems fit with requisite experience in BFSI sector and comply with the SEBI Guidelines /Regulations.

ii) *The* CRAMC shall be under no obligation to act upon the advice rendered by the bidders for the appointment of the CSP. The appointment made by the CRAMC shall be final and binding on all the Bidders.

iii) In case, if there is substantial change in the composition of the Team handling the Cloud Project of the CSP which can significantly affect its execution, the CRAMC reserves its right to penalize the CSP, the proposed rate of penalty would be 0.5% of the entire project cost/TCO per week of delay or non-compliance.

Annexure I

Compliance Requirements (on the letter head of the firm)

Note: The Bidder should mention in seriatim, whether all the compliance are met by marking their responses as 'Y'(Yes) or 'N'(No).

Annexure - I
Cloud Security Assessment Checklist

Introduction

Due diligence while onboarding a cloud vendor is an important step in ensuring that there is no change in the security posture of the Asset Management Company as the vendor will be dealing with business/customer sensitive information protecting which is paramount duty of the Asset Management Company. It is imperative to consider various factors including adherence to industry recognized certifications, rigorous security assessments etc., while onboarding new vendors for the purpose. This document was created with an intent to provide comprehensive list of cloud security considerations as a checklist to be ensured before onboarding a new cloud vendor.

Abbreviation

Abbreviation	Definition/Expansion
CSP	Cloud Service Provider
TSP	Technical Service Provider
MEITY	Ministry of Electronics and Information Technology
IAM	Identity Access Management
CSPM	Cloud Security Posture Management
DPDP	Digital Personal Data Protection Act
CSA	Cloud Security Alliance

Assessment Checklist:

Before onboarding any new cloud vendor, we recommend that the best practices are considered as per various sections of this document and below.

Sl. No	Vendor Compliance Checklist	Compliance Yes/No
1.	The CSP for the deployments should be a MeitY (Ministry of Electronics and Information Technology) empanelled Cloud Service Provider	
2.	Research and assess the potential of the CSP/TSP vendors for their security capabilities and reputation	
3.	Ensure that the CSP is chosen such that CIS Benchmark prescribed configuration recommendations are available in CIS (Centre for Internet Security).	
4.	Blank	
5.	The TSP/CSP to ensure that baseline security configuration of Operating System, Database, Web Server etc. is in accordance with the industry best practices preferably CIS Based benchmark images.	
6.	CSP/TSP should comply to the detailed cloud security best practices published on website of MeitY at following URL: https://www.meity.gov.in/writereaddata/files/2.%20WI3_Cloud%20Security%20Best%20Practices_06112020.pdf	
7.	The data should be stored within geography of India.	
8.	The CSP/TSP to ensure that they would comply to the Reserve Bank of India issued a directive vide circular DPSS.CO.OD. No 2785/06.08.005/2017-18 dated April 06, 2018, on 'Storage of Payment System Data' advising all system providers to ensure that the entire data relating to payment systems operated by them is stored in a system only in India.	
9.	CSP/TSP should ensure establishing necessary DC and DR Setup in multiple seismic zones separated geo-graphical areas or more than 500 kilometres.	
10.	In single region also, multiple availability zones should be available and setup for redundancy and fault tolerance purposes.	
11.	All functions involving critical and PII data to be maintained on-premises only while functions involving noncritical data can be moved to Cloud thereby adopting Hybrid Cloud model approach.	
12.	**Key Management:** The CSP/TSP should provision and utilize management service that stores and manages master encryption keys and secrets for secure access to resources. a. Encryption keys which are used for encryption in cloud should support BYOK (Bring Your Own Keys) and use along with KMS (Key management Service). b. The encryption keys to be exchanged over a secure channel and the keys must be	

	properly secured using KMS and be accessible to the appropriate application/services on a need-to-know basis using properly defined IAM Policies. c. The CSP should support regular rotation of encryption keys and certificates and TSP has to configure accordingly.	
13.	IAM (Identity Access Management) Controls: a. IAM controls, roles, IAM groups, policies to be configured for all the resources, users etc. based on principle of least privilege and are regularly reviewed. b. For administration purposes, privileged accounts, user login and for any critical actions ensure MFA is in place as an additional layer of security of the IAM users and roles. c. Zero Trust security model approach to be ensured.	
14.	Security/Landing Zone: The CSP should have provision for creation and configuring security zones such that resources like computer, networking, object storage, block volume and database resources etc. deployed in such zones comply with well-defined and custom security policies and any violation of policy denies the operation.	
15.	Security Patches and Updates: CSP/TSP should ensure updating their systems/ resources/ application/ instances/ hardware with the latest security patches to maintain a secure Cloud infrastructure.	
16.	CSP should provide secure repository of the digital certificates etc.	
17.	Data Encryption: Ensure data in rest and transit are encrypted with strongest industry standard encryption algorithms.	
18.	The CSP should be able to provide geographic or IP based restrictions.	
19.	Incident response and disaster recovery: Ensure the CSP/TSP has well-defined incident response plan in place to respond quickly and effectively to security incidents and minimize their impact, and regularly test your disaster recovery procedures.	
20.	Data Backup: CSP/TSP should ensure robust, consistent, and regular back-up and recovery/data restoration plans are in place. The data & configuration backups are to be taken in fully encrypted mode and maintained as per the Asset Management Company's policy/procedure.	
21.	Logging and auditing: The CSP/TSP should enable detailed logging and auditing of user, process activities & other activities in all resources including when and how data is accessed, changes in policy assignments, privileged accounts, administration actions and authorization logs which may indicate sensitive or privileged actions, to help detect and respond to security incidents.	
22.	Continuous Monitoring: a. CSP/TSP to ensure continuous monitoring of audit, events, access to critical data and/or processes, or other change/activity logs. b. Asset Management Company Teams also to be given login for dashboard access for checking of the audited logs and security events if required.	
23.	Security Incident Event Monitoring (SIEM):	

	a. The alerts, logs, events from CSPs should be able to integrate with Asset Management Company's incident response process i.e. SOC wherever applicable and/or retention of relevant logs in cloud shall be ensured for incident reporting and handling of incidents relating to services deployed on the cloud. b. The CSP/TSP should establish a dedicated or managed SOC Team for ensuring security incident monitoring on 24x7 basis and effectively respond and remediate to security incidents.	
24.	Cloud Security Posture Management (CSPM): The CSP should support cloud native service that helps Asset Management Company to monitor, identify, achieve, and maintain a strong security posture on the cloud. It should also allow examining cloud resources for security weakness related to configuration, operators, and users for risky activities. Also, upon detection, the native service can suggest, assist, or take corrective actions.	
25.	Data Portability: Ensure that CSP/TSP is flexible by providing suitable options such that data can be easily and seamlessly migrated in case if Asset Management Company decide to switch to another CSP/TSP.	
26.	The CSP/TSP shall ensure for the below. i. The security for hypervisors, containers, and Software defined networks. ii. Proper and adequate incident detection, response, notification, and remediation. iii. Strong perimeter security for API gateways and web consoles iv. MFA v. Assure security isolation between tenants. vi. Configure hypervisors to isolate VMs from each other! vii. Implement processes and technical security controls to prevent admin/non-tenant access to running VMs or volatile memory. viii. Encrypt underlying physical storage. ix. Role based access controls and strong authentication for all container and repository management	

SLAs and Agreements for execution with CSP/TSP

1. The selected vendor shall execute:
   a) Service Level Agreement (SLA), which must include all the services and terms and conditions of the services to be extended as detailed herein, and as may be prescribed or recommended by the CRAMC.
   b) Non-Disclosure Agreement (NDA), the selected vendor shall execute the SLA and NDA within two months the date of acceptance of letter of appointment or as intimated by the Company.
   c) The stamp duty or any other associated charges to execute the above-mentioned document shall be borne by the successful bidder.
   2. Penalty:
      a. CRAMC expects that the selected bidder completes the scope of the project as mentioned. The inability of the selected bidder to either provide the requirements as per the scope or to meet the timelines as specified would be treated as breach of contract

and would invoke the penalty clause. The proposed rate of penalty would be 0.5% of the entire project cost/TCO per week of delay or non-compliance. The company at its discretion may apply this rule to any major non delivery, non-adherence, non-conformity, non-submission of agreed or mandatory documents as part of the Project.

b. Inability of the selected bidder to provide services at the service levels defined would result in breach of contract and would invoke Penalty.

c. The maximum amount that may be levied by way of penalty pursuant to clause above shall not exceed 10% of the Total Contract value.

3. Information Ownership:

All information processed, stored, or transmitted by equipment belongs to CRAMC. By having the responsibility to maintain the equipment, the Bidder does not acquire implicit access rights to the information or rights to redistribute the information. The Bidder understands that civil, criminal, or administrative penalties may apply for failure to protect information appropriately.

While selecting the CSP/TSP and HCISP/TSP, the following security related points are included in the SLA and agreement with the Asset Management Company Ltd.

Sl. No	Vendor Agreement Compliance	Compliance Yes/No
1.	As per the cyber security guidelines by RBI, SEBI and the Regulatory authorities should have access to their IT infrastructure as and when required for audit from security perspective, which may also include visits without prior notice to ensure Asset Management Company's data are not misused	
2.	Ensure third parties/partners/TSP/CSP are also conducting background check, ensuring regular security assessments, audits on their suppliers, vendors, and other third-party partners as well as employees (third-party risk management program)	
3.	Ensure appropriate clauses for not only the uptime, but also for the confidentiality and integrity of the underlying data (For ex. Penalties for every record of a particular type based on sensitivity being exposed or corrupted by a malicious actor)	
4.	Ensure that there is Right to Audit clause in place, in agreement with the vendor/TSP/CSP for performing audit or other assessments & security assessment for the associated infrastructure	
5.	Ensure suitable clauses having the right to monitor and right to terminate services in the event of a security incident or a security breach	
6.	Appropriate clauses may be included in the SLA to protect the interest and to enforce optimum controls as per the Asset Management Company's policy. Vendor/Service provider/TSP/CSP should be bound to a non-disclosure	

	agreement and maintain incident reporting to Asset Management Company in case of any eventuality	
7.	Ensure proper SLAs in place with respect to Data Retention, Masking of Data, Archiving, Destruction of data, Sharing of Data, Encryption of critical data etc.	
8.	The CSP shall adhere to all laws pertaining to data privacy and protection that are applicable as per GOI, RBI and any other regulators	
9.	The CSP shall also ensure that necessary enhancements are made to the services provided whenever there are changes sought either by the regulators or Government of India	
10.	In case of any breach vendor/Service provider should notify Asset Management Company and regulators immediately and provide RCA and take appropriate action, remediate, and cooperate for Incident Management	
11.	**Business Continuity:** The SLA should clearly reflect RTO (Recovery Time Objective) and RPO (Recovery Point Objective), MTD (Maximum Tolerable Downtime), uptime and performance parameters and alternatives for contingency situations for provider infrastructure (including network)	
12.	CSP/TSP vendor has to provide all the Audit Certifications on data center, data security and access control of the cloud deployment	
13.	Ensure proper SLAs in place and certificates are also obtained covering third party vendor/Service/TSP/CSP provider that their systems are at minimum complied to security best practices such as a. Regular conducting VAPT, API Assessment, Source Code audit certified by a CERT-IN empaneled auditor. b. Regular Hardening of System preferably CIS Benchmark, System & Application Patching to latest release patches and security updates c. Adhering to NIST (especially 800-53) and CSF (Cyber Security Framework) standard best practices. d. Monitoring CERT-IN and any other regulator's released advisories and fixing applicable vulnerabilities. e. SOC-II f. **Security Training and Awareness:** The employees as well as vendor staff received security and security awareness training. g. Conduct third party risk assessment on regular basis and monitor for any data breach /leak cases from supply chains to take necessary protective & remedial measures	
14.	**Termination rights and process / Exit strategy:** a. Agreement to consider data deletion including backups and residual data/metadata (ex: system logs, audit logs, access logs, search	

	indices), timelines and written notification of successful deletion. b. Agreement should define exit strategy in the event of termination of the outsourcing agreement. c. Under no circumstances Company shall be liable to the Service Provider for direct, indirect, incidental, consequential, special or exemplary damages arising from termination of this project, even if Company has been advised of the possibility of such damages, such as, but not limited to, loss of revenue or anticipated profits or lost business. d. The company shall have the option to terminate any subsequent agreement and / or any particular order, in whole or in part by giving Vendor at least 90 days prior notice in writing. It is clarified that the Vendor shall not terminate the subsequent Agreement for convenience. e. However the Company will be entitled to terminate subsequent agreement, if Vendor breaches any of its obligations set forth in this RFP and any subsequent agreement and Such breach is not cured within thirty (30) Working Days after the Company gives written notice; or if such breach is not of the type that could be cured within thirty (30) Working Days, failure by Vendor to provide the Company, within thirty (30) Working Days, with a reasonable plan to cure such breach, which is acceptable to the Company. Or Nonconformity of the Deliverables or Services with the terms and Specifications of the RFP as observed during post-delivery audit or otherwise; or Serious discrepancy in the quality of service/hardware/software expected during the implementation, rollout and subsequent maintenance process.	
15.	The agreement shall provide for ensuring prior approval/consent by the Asset Management Company for engaging any outsourcing or sub-contractors by the service provider for all or part of the activity	
16.	The CSP to ensure that the CSP complies with all the necessary security and Data Protection regulations such as Digital Personal Data Protection Act (DPDP), 2023 and the RBI's guidelines on Data Storage and handling	
17.	Ensure that the vendor TSP/CSP/vendors undertakes to remedy any observations reported by RBI/external vendors on cloud operations	
18.	Ensure to provide support/coordinate/undertake necessary activities for smooth transfer of data/applications/APIs in event of reverse migration to on-premises of the Asset Management Company or to any newly selected CSP.	
19.	The CSP/TSP should be able to adhere to the checklist issued by RBI Master Direction dated 10.04.23 on Outsourcing of Information Technology Services (Appendix -I) pertaining to "Usage of Cloud Computing Services"	

20.	The solution provided by the CSP/TSP shall be portable as well as interoperable to any other CSP (data export options need to be considered in case Asset Management Company require migration to another platform)	

Security Solutions in the Cloud

CSP must have the Security Solution capabilities below (an indicative list only) and the TSP should ensure enabling the below Security solutions wherever applicable in the cloud.

Sl. No	Vendor Compliance with Security Solution	
1	Anti-DDOS	
1	WAF	Web Application Firewall
2	SIEM	**Security Information and event management:** The CSP/TSP should establish a dedicated or managed SOC Team for ensuring security incident monitoring on 24x7 basis and effectively respond and remediate security incidents.
3	DAM	Database Activity Monitoring
4	Antivirus Solution & EDR/XDR	
5	PIM (Privileged Identity Management)	
6	API Gateway	
7	Intrusion Prevention System (IPS), Intrusion Detection Solution (IDS), Host Intrusion Prevention System (HIPS)	

Certifications

The cloud service to be availed by the TSP for Asset Management Company shall at least have the following certifications, in addition to MEITY accreditation. They should submit the certificate copy with Bid.

Mandatory certifications to consider – Vendor compliance
ISO 27001 ISMS (Information Security Management System)
ISO 22301 certification (Security and resilience)
PCI DSS (Applicable for storing/processing card transactions and payment information)
SOC II Type 2
CSA Security Trust Assurance and Risk (STAR) Level 2 Certification

Good to have/Preferable certifications to consider – Vendor Compliance
ISO 27017 (Cloud Security Management Certified)
ISO/IEC 27018 (Personal Data in Cloud Certified)

ISO/IEC 27701 PIM (Privacy Information Management) certified
ISAE (International Standard on Assurance Engagements) 3402
SOC III

Security Assessments

Before any application is moved to production, all applicable security assessments shall be undertaken for all the components, services, infrastructure of the application and necessary certificates to be obtained from the CSP/TSP.

In this regard, the CSP/TSP has to undertake on a periodic basis all security assessments on their own or if the Asset Management Company wishes to perform any security assessment as per the SLA.

The details of indicative assessments but not limited to are as per below:

1. End to End Security Assessment
2. Risk Assessments cover a variety of technical, procedural, and human risks.
3. Software Composition Analysis (SCA)

   Assessment using Tools such as 'OWASP Dependency-Check' that actively scans through a project's dependencies to detect and report on publicly disclosed vulnerabilities.
4. Cloud Security Assessment (CSA) for assessing cloud assets and resources for misconfigurations and non-standard deployments not limited to below (including CIS Benchmarks)
   a. Overall security posture
   b. Identity and Access Management
   c. Network security.
   d. Incident management
   e. Storage security
   f. Workload security
   g. Platform services security
5. Container Images Scan & Kubernetes Security Assessment
6. VAPT (Vulnerability Assessment with Penetration Testing) - including CIS Benchmarks
7. Web Application Security Testing (including OWASP Top 10)
8. Secure Configuration Audit
9. Source code audit (SAST - Static Application Security Testing)
10. DAST (Dynamic Application Security Testing)
11. API security assessment for the APIs. (including OWASP Top 10 API)

Note: The security assessments for the above have to be obtained from an independent third-party auditor empaneled by CERT-In.

Annexure-II

Application format for Procurement of Cloud services / Hyper Converged Infrastructure (on the letter head of the firm)

Ref. No. Date:

To,

The Chief Technology Officer,
Canara Robeco Asset Management Company Ltd
4th Floor, Construction House,
No.5 Walchand Hirachand
Marg, Ballard Estate, Mumbai
400001

Sub: Providing Preliminary Information for procurement of Cloud services for Canara Robeco Asset Management Company Ltd.

Dear Sir,

In respect of the procurement of Cloud Services for Canara Robeco Asset Management Company Limited, please find enclosed our response to your RFP dated ……

Having examined the RFP document and the Scope, Eligibility Criteria and other terms and conditions as stipulated therein, we, the undersigned, hereby state that we are in conformity with the specified requirements and would like to offer to provide the Services as defined and described in the RFP, on the terms and conditions mentioned in the RFP Document.

1. We certify that all the information and representations furnished herewith are true, correct, valid and subsisting in every respect and can be supported with relevant documents of proof on demand by CRAMC.
2. We are submitting the application for preliminary evaluation and appointment of our firm for the procurement of Cloud services with regards to Canara Robeco Asset Management Company Ltd and Canara Robeco Asset Management Company and other incidental assignments along with the audit scope.
3. We agree and undertake that if our firm is shortlisted for technical and commercial bidding, we shall comply with the same and undertake assignment as provided by CRAMC SPOC.
4. We agree that 1 bidder will be shortlisted for this activity for a period of 3 years, and we accept that the scope of work, Technical & Functional specifications for the same will be limited to the categories provided in this RFP.
5. If the assignment is awarded to our firm, we agree and undertake to provide the Services comprised in the scope within the timeframe specified, starting from the date of receipt of notification of award from CRAMC.
6. We agree and undertake to abide by the terms and conditions, provisions, stipulations, and covenants from time to time and it shall remain binding upon us and may be accepted at any

time before the expiration of that period.

7. We understand that you are not bound to accept our request for participation in the process or not bound to accept our proposals that you may receive or give any reason for rejection of any application. We also agree and confirm that we will not claim any expenses incurred by us in preparing and submitting this proposal.

8. We are also aware that CRAMC has also right to re-issue / re-commence or completely cancel the selection process, to which we do not have right to object and have no reservation in this regard; the decision of CRAMC in this regard shall be final, conclusive, and binding upon us.

9. We are also aware that in an event of non-performance CRAMC has also right to re-issue / re-commence the selection process, to which we do not have right to object and have no reservation in this regard; the decision of CRAMC in this regard shall be final, conclusive, and binding upon us.

10. The complete set of documents, information about our firm, and clients etc. are enclosed hereto and shall form part of this application.

11. We enclose herewith our firm's profile (as per the prescribed format attached) for your perusal.

12. I/We further declare and confirm that if the assignment is awarded to me/us, it would not result in any conflict of interest either with CRAMC or its Employees, CRMF or its trustees.

I / We confirm that the information furnished here is true to the best of my knowledge.

Thanking you,

Yours faithfully,

Name of the Signatory

Encl: As above

NOTE:

1) All mandatory information requested for as per point No. 2.1 of the RFP should be submitted.

2) Incomplete applications and / or applications not in the prescribed format may be rejected without any further reference.

Annexure-III

Letter of confirmation regarding non-disqualification (to be submitted on letterhead)

Ref. No. **Date:**

To,

The Chief Technology Officer,
Canara Robeco Asset Management Company Ltd
4th Floor, Construction House,
No.5 Walchand Hirachand Marg, Ballard Estate,
Mumbai 400001.

Dear Sir,

With reference to your letter No._____dated_____, I/we confirm as follows: -

i) I am/ Any of our partners is not an officer/employee of your company.

ii) I am/ Any of our partners is not a partner or in employment of any office or employee of your company.

iii) I am/ Any of our partners or Associates firms or sister concern or Branch office, is not assigned with any ongoing information security activity for your company.

iv) I am/ We are not otherwise disqualified by SEBI, RBI, Canara Bank and its associates and subsidiaries.

v) I/ We also confirm that I am/we are full time practicing information security firm and am/are not employed elsewhere and do not have any other business interest.

vi) I/ We also assure you that I/ we will not be disqualified during the course of the assignment for any of the reasons mentioned above.

vii) I/ We undertake not to subcontract any activity mentioned in the SOW assigned to me/us to any outsider without the express consent from CRAMC.

Yours faithfully,

Name of Signatory

Annexture IV - RFP Specification - Canara Rebeco-v1.0.1.xlsx attached.