Request For Proposal (RFP)

For

SELECTION OF Managed Security Services

FOR

COMPREHENSIVE INFORMATION AND APPLICATION SECURITY ASSESSMENT

Information Security Department
Canara Robeco Asset Management Company Ltd.

Construction House, 4th Floor, 5, Walchand Hirachand Marg, Ballard Estate,
Fort, Mumbai, Maharashtra 400001

17th day of May, 2022

Important Note: Applications in response to this RFP are invited to carry out a preliminary evaluation to assess the suitability of the applicants 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.

Disclaimer

The information contained in this RFP document or information provided subsequently to applicants whether verbally or in documentary form by or on behalf of Canara Robeco Asset Management Company Limited (CRAMC), is provided to the applicant(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 applicants who are qualified to submit the applications as per the eligibility conditions. The purpose of this RFP is to provide the applicant(s) with information to assist the formulation of their proposals. This RFP does not claim to contain all the information each applicant may require. Each applicant 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 an Applicant may require. CRAMC does not undertake to provide any applicant 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 applicants. 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 the expression 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.

Canara Robeco Asset Management Company Ltd

Invitation of Tender Offers

1. Invitation for appointment

1.1. Canara Robeco Asset Management Company Ltd (CIN: U65990MH1993PLC071003) a company incorporated under the Companies Act 1956 having its Registered and Corporate Office at 4th Floor, Construction House, No.5. Walchand Hirachand Marg, Ballard Estate, Mumbai 40001, hereinafter referred to as "The Company" invites sealed tender offers in the prescribed format (Attached as **Annexure-II**) from eligible, reputed entities for Empanelment of Service Provider for conducting Application Security review, Vulnerability Assessment and Penetration Testing of Internet facing Applications and Infrastructure, SAS Platform Review, Office365 Penetration Testing, API Security Review, Mobile Applications – SAST and DAST based review, Network and Cloud Architecture Assessment, Firewall Rule Review and Red Team Assessment. In this RFP, the term bidder/prospective bidder refers to the primary bidder participating for delivering services mentioned in the scope of works.

Important Note: Based on our internal norms, bidding firms not exceeding five will be shortlisted for the purpose of technical and commercial bidding process.

1.2 Due Diligence

The Applicant 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 applicant's risk and may result in rejection of the Application.

1.3 Cost of Participation

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

1.4 Clarification of RFP Documents

A prospective Applicant requiring any clarification on this RFP may contact CRAMC in writing by E-mail at **infosec.ciso@canararobeco.com**. CRAMC shall respond in writing by E-Mail to any request for clarification of the application documents, from the prospective applicants, which it receives not later than 20.05.2022. 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.

1.5 Amendment of RFP Document

a) CRAMC reserves the sole right for including any addendum to this entire selection process. The applicants shall not claim as a right for requiring CRAMC to do the aforesaid.

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 applicants, modify this RFP Document.

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

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

1.6 The hard copy of the application duly signed and stamped along with supporting documents should be submitted in a sealed cover to the following address:

Chief Information Security Officer,
Canara Robeco Asset Management Company Ltd,
4th Floor, Construction House,
No.5, Walchand Hirachand Marg,
Ballard Estate, Mumbai 40001.

and sent by postal service/courier/hand delivery duly superscribing the envelope **"Application for SELECTION OF SERVICE PROVIDER FOR COMPREHENSIVE INFORMATION AND APPLICATION SECURITY ASSESSMENT**."

1.7 The proposed appointment would be for two financial years (i.e. from April 01, 2022 to March 31, 2024) and shall be renewed for a further period subject to review by CRAMC.

1.8 Last date for submission of the applications with all relevant documents in a closed cover is 27th May 2022 by 6.00 PM. Applications received thereafter shall not be considered.

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

1.10 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.

2 **Information Required**

2.1 Mandatory information to be submitted on the letter head of the firm to be eligible for the bidding process (Please attach as Annexure 1):

Sr.No.	Particulars	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.	Company Head Office Address	
6.	Registered Office Address	
7.	GST Number	
8.	Whether the Firm or any partner has ever been debarred by RBI/CAG/or any Government Organization if yes, details: Regn.No. Name of the partner Brief reasons for debarment	
9.	Whether Registered/ empaneled with RBI/ CAG/SEBI/Certin, if yes give the details	
10.	Whether your firm had or is presently having any kind of professional/business association directly with Canara Bank, Orix Corporation (Japan) or Robeco Group NV (Netherlands) or any of their associates in India or elsewhere, which is likely to result in conflict with the proposed assignment under this RFP?	
11.	Name, Designation, Tel. No, E-Mail of the authorized signatory submitting the RFP (Please enclose the copy of board resolution)	
12.	Any pending or past litigation (within three years)? If yes please give details	
13.	Turnover for past 3 years (FY, Turnover, Net Profit, Net Worth)	
14.	Brief profile of Partners/Director in the following manner)	

Name/ Qualification	**Total Experience**	**Experience with Current firm**	**Whether CISSP / CISA**	**Mobile No.**

13.	Past Experience of similar Experience

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

3. Documents to be submitted with the application

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) Registration/empanelment certificate/letter issued by RBI/CAG/SEBI.
vi) CERT-in empanelment
vii) Scope along with sampling criteria for various areas of control presentation regarding approach & deliverables in case of clarification vendor must be requested to present their approach in CRAMC office.
viii) Letter of confirmation regarding non-disqualification as per Annexure - III

4 **General Conditions**

i.	No communication will be sent by the CRAMC and no correspondence will be entertained in respect of firms, which are not being selected.
ii.	The selected Firm, on receiving the offer letter from CRAMC, shall submit the 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 carried out 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 applicant'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 discretion of CRAMC and no rights whatsoever accrue to the firm for such appointment.
vi.	The selected firm will have to stick to the following deadlines: - Credential based assessment of all Critical Applications like Website, Mobile app, Critical Apis (5 apis), External Public IP Scan for vulnerabilities, Black box testing of all internet facing platforms – Quarterly Basis and submit report - All Other Penetration Testing, Vulnerability Assessment, Open-Source Assessments, Firewall Rule Review, PAM Solution Review, VMWare Review, Cloud Environment review,

	Configuration Review of Critical Security Platforms, Cryptographic Control Review, and Network Architecture Review once in six months - Red Team Assessment, Risk Assessment of Security Platforms, Data and Database Security Assessment - Identify collect and Review Security Documents Annually - Provide Annual Improvement Plan
ix.	The firm shall adhere to the coverage strictly as per the scope as may be decided by CRAMC from time to time.
x.	CRAMC reserves the right to seek views from the entities with whom the firm is/has been/was associated.
xi.	The firm shall not sub-contract without the express permission from CRAMC, part of the scope of work assigned to any outside firm or other persons.
xii.	Any other terms and conditions of the assignment would be decided by CRAMC on a case-to-case basis.

5. Tenure of Assignment

CRAMC will appoint two firms for two financial years. The term may be extended, solely at the discretion of CRAMC on satisfactory review by the competent authority.

6. Important information about other expenses

a. No travelling allowance/ halting allowance shall be paid to the bidder for carrying out the assignment.

b. Payment to the bidders will be exclusive of tax.

c. The Assessment charges once fixed shall remain unchanged throughout the tenure of 2 years. CRAMC's decision will be final in this regard.

7. Conduct and Performance Monitoring

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

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

c. CRAMC reserves its right to review the appointment at any point of time and if necessary, to cancel the appointment by giving 7 days' written notice. In case of termination of assignment, the remuneration for the incomplete month and the residual period of engagement shall not be payable by CRAMC.

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

e. The Bidders are expected to provide an executive summary of observations along with every report and submit the same to the Chief Operating Officer.

8. Representations and Warranties

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

b. That the Applicant 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 Applicant 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 Applicant shall be bound by all the terms of the RFP.

d. That the Applicant 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 Applicant 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 Applicant 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.

vi. That the Applicant 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 liens thereon and shall keep CRAMC, its directors, officers, employees, representatives, consultants and agents indemnified in relation thereto.

vii. That all the representations and warranties as have been made by the Applicant 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.

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

ix. That there are – (a) no legal proceedings pending or threatened against Applicant 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 Applicant or any of its Partners or its team members by any statutory or regulatory or investigative agencies.

x. That the Applicant 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.

xi. That all conditions precedent under the Engagement have been complied.

xii. That neither the execution and delivery by the Applicant of the Engagement nor the Applicant'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, writ, injunction or decree of any court or governmental authority binding on the Applicant (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 Applicant is a party or by which it or any of its property or assets is bound or to which it may be subject.

9 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 Confidentiality Agreement prior to finalization of Engagement and shall abide by the terms and conditions of confidentiality as contained therein.

10 Governing Law

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

11 Jurisdiction of Courts

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

12 Time Limit for the Commencement of Work

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

Annexure I

Broad scope of Work for Managed Security Services

<table>
<tr><th>Scope of Work</th><th>Description of the scope</th></tr>
<tr><td>Category</td><td>
<table>
<tr><th>Sr. No.</th><th>Category</th><th>Scope</th></tr>
<tr><td>1</td><td>Category 1</td><td>Red Team Assessment, Internal Risk Assessment, Policy and Procedure Review, Security Tools Configuration Assessment, Firewall Rule Review, Hardening Documents, Cyber Maturity Assessment, Phishing Activity,</td></tr>
<tr><td>2</td><td>Category 2</td><td>VAPT of Mobile and Web Applications, API Security Testing, Wi-Fi Assessment, External Threat Assessment, Dark Web Threat Assessment, VA of Internal Systems, Cloud Security Assessment, Source Code Review (DAST,SAST),</td></tr>
</table>
</td></tr>
<tr><td>1) Category 1</td><td>1.1 Successful Bidder will have to conduct at least one Red Team Assessment activity as communicated by the CRAMC SPOC annually and report the same
1.2 Annual Risk Assessment to be conducted on the Internal Risks identified by the Security Vendor. This assessment will include identification and mitigation of IT Security gaps, Prevention of Data Breaches, Asset Criticality Assessment, Identification of OS tools, Identification of out of support assets and tools, Forecasting of Security requirements, Network Architecture Review
1.3 Annual Evaluation of all Policies and Procedures related to Information Security
1.4 Configuration Assessment and compliance of all Information Security Devices including Cloud infrastructure will be conducted once in six months
1.5 Firewall Rule Review will be conducted at least once every 4 months
1.6 Hardening of entire Infrastructure relating to CRAMC Servers - 5, Network, Security devices & system - 10, Annual review and updating of hardening documents
1.7 Annual Cyber Maturity Assessment
1.8 At least one phishing activity every 6 months</td></tr>
<tr><td>2) Category 2</td><td>1.1. Vulnerability Assessment and Penetration Testing of entire Infrastructure relating to CRAMC Network, Data Centre, DR Site, and Branches to be conducted once in 6 months. Security Configuration review to conduct once in a year.</td></tr>
</table>

	1.2. Every VA&PT shall have two test cycles one at the beginning of VA&PT for identification of gaps and to check for known vulnerabilities, and a retesting post closure of vulnerabilities identified 1.3. VA&PT of critical applications shall be conducted Quarterly in every financial year. The remaining applications shall be conducted twice in a year cycle. 1.4. VA&PT of critical internet facing applications and Infrastructure components shall be conducted at least once in 3 months. All other applications once in six months 1.5. An assessment of the need for security testing shall be conducted whenever any change is made to any internet facing applications or to any infrastructure component irrespective of the magnitude of change 1.6. Mandatory security testing shall be conducted in case of all applications and related infrastructure components so as to check for known vulnerabilities once initially and again whenever major changes in internet facing applications and related infrastructure components take place. However, all Internet facing applications shall be tested for all major and minor changes either through internal or external VA, and any gap found shall have to be disclosed. 1.7. The entire VA&PT exercise will be a combination of Blackbox and Grey Box Testing only 1.8. External Vulnerability scanning will be conducted on a monthly basis and a report will be submitted for the same 1.9. The VA&PT activity will also consist of MFA testing, VPN Security Testing, Office365 Controls security testing 1.10. Successful Bidder will have to conduct at least one Dark Web Threat Assessment for CRAMC Footprint every 6 months 1.11. Cloud Security Assessment of Cloud Architecture, Vulnerabilities and Configuration to be conducted at least once in 6 months including Office365 cloud 1.12. Annual Source Code Review to be conducted DAST or SAST on critical applications 1.13. API Security Testing to conduct twice in a year 1.14. Wi-Fi Assessment to conduct twice in a year

Annexure-II

FORMAT FOR APPLICATION FOR APPOINTMENT OF Information Managed Security Services (on the letter head of the firm)

Ref. No. Date:

To,
The Chief Information Security 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 appointment of Managed Security Services Provider(MSSP) for Canara Robeco Asset Management Company Ltd for the FY 2022-24

Dear Sir,

In respect of the appointment of MSSP 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 MSSP assignments with regards to Canara Robeco Asset Management Company Ltd and Canara Robeco Mutual Fund and other incidental assignments along with the audit scope.
3. We agree and undertake that if our firm is short listed for technical and commercial bidding, we shall comply with the same and undertake assignment as provided by CRAMC SPOC.
4. We agree that 2 bidders will be shortlisted for this activity for a period of 2 years and we accept that the scoping for the same will be limited to the categories provided in this RFP. This will be interchanged annually between the shortlisted vendors.
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 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 entire 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 are 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 format may be rejected without any further reference.

Annexure-III

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

Ref. No. **Date:**

To,
The Chief Information Security 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 from 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 confirm 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