



REQUEST FOR PROPOSAL

For Comprehensive Security Review of Applications

Reference Number: SBIS2425RMDHS008

**State Bank of India, Risk Management Department,
#27-01, 80 Robinson Road, Singapore, 068898**

1. SCHEDULE OF EVENTS

Bid Details Availability	Document carrying the details about the RFP and Bidding can be downloaded from website (https://sg.statebank/) under the procurement section) from 07:30 PM on 28.11.2024 until 1:00 PM on 18.12.2024 .
Last date for requesting clarification (optional)	Up to 1:00 PM on 18.12.2024 All clarifications/queries regarding RFP points / clauses requiring clarifications may be sent by e-mail to “ avpit.security@sbising.com ”. The format for pre-bid queries is placed as Annexure D . The email ID avpit.security@sbising.com is solely to be used for seeking the clarification and no bids shall be submitted to the same email address.
Date and Time for submission of Bids	All bids in a password protected document are to be mandatorily submitted via email to “ ittender@sbising.com ” only in between 03:00 PM - 5:00 PM only on 18.12.2024 (Refer section 6). Bids shall only be submitted to the email address “ ittender@sbising.com ”
Date and Time for submission of Passwords	Passwords are to be mandatorily submitted via email to “ ittender@sbising.com ” in between 05.00 PM - 07:00 PM only on 18.12.2024 (Refer section 6).
Opening of Technical & commercial Bids	19.12.2024
Address for Communication and submission of bid.	AVP (Cyber Security Operations), Risk Management Department, State Bank of India, #27-01, 80 Robinson Road, Singapore, 068898
Telephone	+65-62222033
All bids relating to this RFP should be sent to following email id	ittender@sbising.com

2. INVITATION TO BID

- i. State Bank of India (hereinafter referred to as SBI / the Bank) is having its Corporate Centre at Mumbai and other offices in various cities across India and in 36 Countries.
- ii. In order to meet the security requirements of State Bank of India, Singapore Office, the Bank proposes to invite tenders/proposals from established organizations (hereinafter referred to as “bidder”) to undertake comprehensive security review of applications as per scope details listed out in the **Annexure-A** of this document.
- iii. The bidding document carrying details related to RFP may be obtained from the Bank as under or could be downloaded from Bank’s Website <https://sg.statebank/> under the procurement section (<https://sg.statebank/procurement>). The password protected bids shall be submitted to the bank only as per **Section 6 (Submission of Bid)** of this document.
- iv. Please note that all the information desired needs to be provided. Incomplete information and/or Unsigned Unstamped proposals may lead to non-consideration of the Proposals/Quote.
- v. Bank reserves the right to change/extend at any time, the dates mentioned in this RFP document, which will be communicated to the bidders through our website only.
- vi. The information provided by the bidders in response to this RFP document will become the property of SBI and will not be returned. SBI reserves the right to amend, rescind or reissue this RFP and all amendments will be advised to the bidders through our website only and such amendments if any will be binding on them.
- vii. Quotes received before or after the aforesaid date and time will not be entertained for evaluation and shortlisting.
- viii. Unsigned/ Incomplete Quote, Unstamped Quote and those which are not signed by authorized signatory may not be entertained for evaluation and shortlisting.
- ix. All clarification to be sought through email to “avpit.security@sbising.com” quoting the Reference number stated above and **Bids must only** be submitted to the email address “ittender@sbising.com”.

3. DISCLAIMER

- i. The information contained in this Request for Proposal (RFP) document or information provided subsequently to bidder(s) or applicants whether verbally or in documentary form/email by or on behalf of State Bank of India (Bank), is subject to the terms and conditions set out in this RFP document and all other terms and conditions subject to which such information is provided.
- ii. This RFP is neither an agreement nor an offer and is only an invitation by the Bank to the interested parties for submission of bids.
- iii. The purpose of this RFP is to provide the Bidder(s) with information to assist preparation of their proposals/quotations. This RFP does not claim to contain all the information each Bidder may require. Each Bidder should conduct its own investigations and analysis and should check the accuracy, reliability and completeness of the information contained in this RFP and where necessary obtain independent advices/clarifications. Bank may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP.
- iv. The Bank, its employees and advisors make no representation or warranty and shall have no liability to any person, including any Bidder under any law, statute, rules or regulations or tort, principles of restitution or unjust enrichment or otherwise for any loss, damages, cost or expense which may arise from or be incurred or suffered on account of anything contained in this RFP or otherwise, including the accuracy, adequacy, correctness, completeness or reliability of the RFP and any assessment, assumption, statement or information contained therein or deemed to form or arising in any way for participation in this bidding process.
- v. The Bank also accepts no liability of any nature whether resulting from negligence or otherwise, howsoever caused arising from reliance of any Bidder upon the statements contained in this RFP.
- vi. The Bidder is expected to examine all instructions, forms, terms and specifications in this RFP. Failure to furnish all information required under this RFP or to submit a Bid not substantially responsive to this RFP in all respect will be at the Bidder's risk and may result in rejection of the Bid.
- vii. The issue of this RFP does not imply that the Bank is bound to select a Bidder or to award the contract to the Selected Bidder, as the case may be, for the Project and the Bank reserves the right to reject all or any of the Bids

or Bidders without assigning any reason whatsoever before issuance of purchase order and/or its acceptance thereof by the successful Bidder as defined in Award Criteria and Award of Contract in this RFP.

4. Scope of Work

Following Applications shall form the broad level scope:

1. Enterprise Remittance System
2. Online Remittance System
3. Thomson Reuters Trade Platform
4. FAST
5. Lexis Nexis Name Screening
6. Myinfo
7. MEPS+
8. Onfido
9. CTS/G3
10. Thales RBA

Details of the scope is provided in the **Annexure-A** of this document.

5. ELIGIBILITY AND TECHNICAL CRITERIA:

Bid is open to all Bidders who meet the eligibility and technical criteria as given in **Annexure-B & Annexure-C** of this document. The Bidder has to submit the documents substantiating eligibility criteria as mentioned in this RFP document.

6. SUBMISSION OF BID

The bidders shall submit the undermentioned password protected files via email to "ittender@sbising.com" in between **03:00 PM - 5:00 PM on 18.12.2024 only (Singapore Standard Time)**.

- a. **Technical Bid File:** Carrying the details of the solution proposed along with brief history of the firm, its existing customers, clients and businesses, registration document of the firm and along with confirmation on eligibility criteria as detailed in **Annexure-B**.
- b. **Financial Bid File:** Carrying the detailed costing of the security review cost. The same should be submitted as per the template provided in **Annexure-G**.

- c. The password of the aforementioned files to be shared via email to “ittender@sbising.com” in between **05:00 PM - 7:00 PM on 18.12.2024** only (Singapore Standard Time).
- d. Quotes received before or after the aforesaid date and time may not be entertained for evaluation and shortlisting.
- e. Unsigned/ Incomplete Quote, Unstamped Quote and those which are not signed by authorized signatory may not be entertained for evaluation and shortlisting.
- f. All clarification to be sought through email to “avpit.security@sbising.com” quoting the Reference number stated above and **Bids must only** be submitted to the email address “ittender@sbising.com”.

7. Bid Prices

- a. Prices are to be quoted strictly in **Singapore Dollar** only.
- b. Prices quoted should be inclusive of all Government levies, excise duty, custom duty, etc., as also cost of incidental services such as transportation, insurance etc. but exclusive of Goods & Service Tax (GST) payable.

8. Delivery Schedule & Penalty for Delayed Deliveries

- a. Delivery of all the requested reports after completion of the review should be completed within requested timelines.
- b. The Bank also reserves the right to cancel the Purchase Order. In the event of such cancellation, the vendor is not entitled to any compensation. Please note the delivery schedule shall be followed strictly as stipulated. Any delay shall be viewed seriously and penalties levied.

9. Deadline for Submission of Bids

- a. Signed and completely Bids/Quote must be received by the Bank at the specified email address (i.e. ittender@sbising.com), no later than the date & time specified in the “Schedule of Events” in Invitation to bid.

10. Contacting the Bank

- a. No bidder shall contact the Bank on any matter relating to its Bid, from the time of submission of Price Bid to the time the Contract is awarded.
- b. Any effort by a bidder to influence the Bank in its decisions on Bid evaluation, bid comparison or contract award may result in the rejection of the bidder's bid and consequent black listing for future contracts for a period of no less than 3 years.

11. Award Criteria

- a. The evaluation of bids will be conducted based on the combined assessment of the technical and commercial proposals. The bidder whose proposal demonstrates the best overall suitability, considering both technical and commercial aspects, shall be selected as the successful bidder. The decision will be based on the following:
 - i. Technical Evaluation: Proposals will be assessed against the technical requirements and criteria outlined in the RFP. Only bidders meeting the minimum technical qualification score will be considered for further evaluation.
 - ii. Commercial Evaluation: Commercial bids of technically qualified bidders will be opened and evaluated to determine the most competitive pricing.
 - iii. Overall Suitability: The bidder with the best combination of technical and commercial scores, aligning with the objectives of this RFP, will be deemed most suitable and awarded the contract. The final decision of the successful bidder will be at the sole discretion of the Bank, ensuring alignment with the project's goals and requirements.

12. Bank's right to accept any bid and to reject any or all bids

- a. The Bank reserves the right to accept or reject any Bid in part or in full or to cancel the Bidding process and reject all Bids at any time prior to contract award, without incurring any liability to the affected bidder or bidders or any obligation to inform the affected bidder or bidders of the grounds for the Bank's action.

13. Notification of Award

- a. Prior to expiration of the period of Bid validity, the Bank will notify the successful bidder in writing or by e-mail, that his Bid has been accepted.
- b. Only the notification of award will not constitute the formation of the Contract. The selected bidder should convey acceptance of the award, SLA and NDA within 7 days of receipt of the communication or a through a confirmation mail. By submitting their proposals, the bidder agrees to comply with the SLA terms which shall be stipulated by the Bank, with no material deviations permitted. The detailed template of the Service Level Agreement (SLA) will be provided to the successful bidder upon award of the contract. The final SLA will form an integral part of the contract and must be signed by the successful bidder prior to the commencement of services.
- c. Upon notification of award to the selected bidder, the Bank will promptly notify unsuccessful bidder either through email or notice on website.

14. Non-Disclosure Agreement

- a. The successful Bidder will have to submit Non-disclosure Agreement as desired in this RFP and strictly on the lines of format given in Annexure E of this RFP.

15. Inspection and Quality Control Tests

- a. The Bank reserves the right to carry out inspection at successful bidder's office by a team of Bank officials or an auditor appointed by the Bank.

16. Subcontracting:

As per scope of this RFP, sub-contracting is not permitted.

17. Payment Terms

- a. Payment shall be made in Singapore Dollar. 100% amount will be released on receipt of final report post confirmatory scan. Details are provided in the Annexure-A.

18. Prices

- a. Prices payable to the Vendor as stated in the Contract shall be firm and not subject to adjustment during performance of the Contract, irrespective of reasons whatsoever, including exchange rate fluctuations, changes in taxes, duties, levies, charges, price inflation etc.
- b. The Bank reserves the right to re-negotiate the prices in the event of change in the international market prices, industry best practices etc. of such services.

19. Change Orders

- a. The Bank may, at any time, by a written order given to the Vendor, make changes within the general scope of the Contract in any or entire scope before delivery of service.
- b. If any such change causes an increase or decrease in the cost of, or the time required for the Vendor's performance of any provisions under the Contract, an equitable adjustment shall be made in the Contract Price or delivery schedule, or both, and the Contract shall accordingly be amended. Any claims by the Vendor for adjustment under this clause must be asserted within thirty (30) days from the date of Vendor's receipt of Bank's change order.
- c. The Bank reserves the right to withdraw this RFP anytime without any prior notice.

20. Applicable Law:

The Contract shall be interpreted in accordance with the laws of the Republic of Singapore and shall be subject to the exclusive jurisdiction of courts at Singapore.

Addresses for Notices

The following shall be the address of the Bank and Vendor.

Bank's address for notice purposes:

State Bank of India, Risk Management Department, #27-01, 80 Robinson Road, Singapore, 068898

Vendor's address for notice purposes

'Registered address as available in ACRA / Applicable Registration document' on the date of the notice.

Annexure-A**DELIVERABLES/SCOPE OF WORK****Comprehensive Security Review (CSR) of Applications****Scope:**

Number of Applications	10
Type of Applications	Web Based-06 API Based-03 Thick Client-01 Total-10
Exposure	Internet- 01, Intranet-09
No of Devices for VA and SCD Review	OS-36, Database-11, App-15, Web-09 (Total 71)
Source Code Review	Lines of Code- 1,00,000 Programming Language- .Net Framework
Application Security Review	Number of User Roles-20 Input/Dynamic Pages-300
Number of Firewall Rules	65
Number of APIs Hosted	05

The Major Scope of the Security review of Applications is summarized below:

a) Secure Network Architecture Review

- a.1 Placement & Security of servers & network devices in SBI Network
- a.2 Firewall Rule Base Review
- a.3 Analysis of traffic monitoring (inward and outward traffic)

b) Application security review

- b.1 AppSec of application
- b.2 Role based Application review

c) VA/PT of all the Assets in scope

- c.1 VA – all the ports Internal, Credential Based
- c.2 Both Internal and external PT

d) Configuration Audit

- d.1 Configurations of All components such as OS, Database, Application server, web server etc. need to be reviewed (script based or manual) against Bank's Benchmark Document.

e) Process Review: Process flow including.

- e.1 User management, privilege access etc., change control management, generation and checking of logs, incident management, flow of both to & from traffic (its contents and the format in which it is travelling), storage at any point, password management, security environment, Compliance with RBI and local regulatory guidelines and Local Privacy Law and Bank's IT Policy and IS Policy and industry best practices.
- e.2 Assessment of security risk involved in data being processed/handled at third party vendor's site/location covering end to end data flow to ensure CIA of information.
- e.3 Review of each Database-on-database security perspective.
- e.4 Review of Vendor/ Third Party Access management
- e.5 In view of a few Applications under scope are with third party vendors, the selected ISSP must review the controls implemented by the vendor for Bank's Data processing as against Bank's set-in controls at third party data processing of Bank's data.
- e.6 Data Flow Diagram for all the Applications to be obtained and 'end to end' process review, specifically on third party locations, if any need to be carried out.

f) Source code review – Source code review wherever applicable.

g) API Review: API review.

h) Digital Forensic Readiness Assessment: Assessment of Forensic readiness and threat intelligence for individual Applications.

i) Compliance Review – as per Bank’s IS Guidelines, Cyber Security Policy, Regulatory Guidelines and Best Global Security practices. Comprehensive Review of approximately 80 control points of the Bank’s IS Guidelines will be required to be carried out. These control points shall be related with areas like- Governance, Asset Management, Infrastructure Security, End-Point Security, Application Security, Server Room/ Data Centre Security, Network Security, ATM Security, Supply Chain Security, Data Security, Human Resource Security, Business Continuity Management etc.

j) Preparedness for Ransomware:

- j.1 Assessment of Backup process
- j.2 Evaluation of enforcement of the defined back up process and Restoration testing.
- j.3 Compliance on patch management.

k) Data Security

- k.1 Assessment of Backup process
- k.2 Evaluation of enforcement of the defined back up process and Restoration testing.
- k.3 Compliance on patch management.

l) Supply Chain Risk Management (SCRM)

Artefact Based review of Supply Chain Risk Management will have to be carried out for the following third-parties:

Name of Third-Party Vendor	Services Offered/ Purpose of Integration
Myinfo	KYC
MEPS+	Transaction Processing
FAST	SGD to SGD transaction Processing
Onfido	E-KYC
CTS/G3	Cheque clearing and Giro Transaction Processing
Thales RBA	Fraud monitoring

Deliverable for the Engagement:

1. Hash Value and version number of every application (as advised by the Application Owner and for which it was reviewed) will be required to be incorporated in the final report for both initial and confirmatory review.
2. Detailed Report highlighting vulnerabilities in the system. Technical vulnerability identified should provide: Risk impact (High, Medium, Low), possibility of occurrence (High/Medium/Low), ease of exploitation (Easy/Difficult/Very Difficult), specific mitigation measures keeping in view the criticality of the application, placement of the systems, type of the information passing over the channel, compensatory controls etc. If the service is vulnerable, screen shot/logs depicting vulnerability and change required in Secured Configuration Document may also be suggested.
3. If any observation has been made which is as per the global best practices and not included in the Bank's latest policies, Regulatory guidelines, the relevant reference will have to be provided in the report by the ISSP.
4. Both initial and final reports (after completion of the confirmatory review) will have to be presented application wise.
5. A summary report (component wise) for all the applications/review areas (combined) will also be a part of both the reports.
6. Both safe as well as unsafe findings are required to be listed along with the Mitigation tracker, listing the unsafe findings.
7. An application and activity wise daily tracker to be provided to the IT and Risk Management Departments.
8. Recommendations for risk containment based on global best practices, Compliance to the Bank's latest Policies, regulatory guidelines etc. requirements would be required to be evaluated and reported.
9. 100% confirmatory review will be required to be conducted. However, if the 100% confirmatory is not covered in first round, the Bank reserves the right to call the ISSP team to conduct other round(s) of confirmatory test, under prior intimation, if required, without any extra cost.
10. Along with the soft copy of the final report, its printout with all pages signed by the authorized signatory under your company's seal must be submitted. The complete report should contain the following information also: -

Date of report

- i Exact period of conduct of the review and/or confirmatory review (as the case may be)
- ii Running page number for all pages
- iii Name and designation of the officials from IT and Risk Management departments with whom the findings had been discussed and finalized.
- iv If the ISSP resource is required to visit Bank's vendor partner's premises and/or for conducting White Box testing of the Source Code, the NDA will be signed between the ISSP resource and the Bank's vendor partner invariably.
- v E-Mail response from the Application Owner team may suffice in most of the cases of any reference in respect of the observations made. However, if required, the ISSP resource will be required to visit Bank

premises for a one-on-one interaction on one or more instances with the Application Owner and/or Information Security Department.

- vi ISSP to suggest risk containment / risk mitigation controls in case some of the remediation suggested in the report cannot be implemented because of technical or business-related reasons-application dependency.
- vii **Delivery Schedule:** The initial review is to be completed and report to be submitted within 3 months from the date of Purchase Order. In case, after selection of L-1 ISSP, there is a delay in placing the formal Purchase Order, the Bank may provide a mail confirmation that the ISSP has been selected by the Bank for conducting the captioned review and the review process may be started on a notice of one day (formal Purchase Order may be placed by the Bank later).
- viii All the payments shall be made by the Bank to the Selected Bidder except as otherwise provided in the bid after deducting all taxes, as per laid down provisions from time to time. All the payment shall be in Singapore Dollars. The detailed payment terms are given below: -

S. No.	Description	Terms of Payment
1	After submission of Reports of 1 st Round of Review	70%
2	After submission of Reports of Confirmatory Review	30%

**The initial review has to be completed within three months of the project inception.

Confirmatory Review: If 100% compliance/closure of observations is not achieved in first round, the ISSP must do subsequent confirmatory reviews till the 100% closure of the observations.

Annexure-B

Eligibility Criteria

Applicants must read carefully the conditions of eligibility criteria provided herein. Bidders meeting the eligibility criteria are eligible to submit their bids along with supporting documents. Bid is subject to rejection, if not accompanied by required documents supporting the eligibility criteria. To be eligible for evaluation of its Proposal, the Applicant shall fulfil the following:

Sr. No.	Eligibility Criteria	Compliance Y / N	Documents to be submitted
1.	The bidder should have minimum 3 years of experience in the area of IT and Cyber Security.		Copy of the company registration from appropriate authorities and certifications & accreditations to be provided. Details to be provided as per the template annexed (Refer Annexure F1) .
2.	The bidder should have performed at least 2 Comprehensive Security Review/ Exercise of similar scale for Banks/Financial Institutions during the last 24 months.		Bidder to provide the details of such engagements along with client copy of order. Details to be provided as per the template annexed (Refer Annexure F2) .
3.	The bidder should use only licensed software for testing and scanning the Bank Infrastructure. Following category of tools shall not be allowed by the Bank: <ul style="list-style-type: none"> • Open Source • Cloud based tools 		Bidder to provide the undertaking on bidder's letter head duly signed by the Authorized signatory of the firm/company confirming that Open Source and Cloud based tools will not be used. An undertaking to be provided as per the template annexed (Refer Annexure F3) .
4.	Any entity which has been barred by the Central Government, any State Government, a statutory Bank, public/private sector bank or a public sector undertaking, as the case may be, from participating in any		Bidder to provide the undertaking on bidder's letter head duly signed by the Authorized signatory to confirm that no past/present litigations exists against the company/firm. An undertaking to be provided as per the

Sr. No.	Eligibility Criteria	Compliance Y / N	Documents to be submitted
	project, and the bar subsists as on the date of Proposal, would not be eligible to submit a Proposal either by itself or through its Associate.		template annexed (Refer Annexure F3).
5.	An Applicant or its Associate should not have been declared ineligible for corrupt and fraudulent practices by the Govt. / State Governments / Regulatory Agencies/ PSU/ Bank/ Private Company.		Bidder to provide the undertaking on bidder's letter head duly signed by the Authorized signatory confirming that the company/firm has not been declared ineligible for deficiency in Service, or for corruption and fraudulent practices by Government / any State Government / Regulatory Agencies / Public Sector Undertaking/ any Bank / Private Company. An undertaking to be provided as per the template annexed (Refer Annexure F3).
6.	The bidder should have at least 10 expert/certified resources at Singapore location with any of the following certifications: <ul style="list-style-type: none"> a. CISA b. CISSP c. CCNA d. CISM e. CEH f. ISO 27001 Lead Auditor g. Certified Cyber Forensic Professional (CCFP) h. SSCP i. OSCP j. Crest Practitioner Security Analyst (CPSA) k. Crest Registered Penetration Tester 		Bidder to provide the details (Name of Employee, Professional Experience in years, Certification) as annexure in a tabular format

Sr. No.	Eligibility Criteria	Compliance Y / N	Documents to be submitted
	l. OSCE m. GSEC n. GCIA o. GCIH		
7.	Subletting or outsourcing is strictly prohibited.		Bidder to provide the undertaking on bidder's letter head duly signed by the Authorized signatory to confirm that no subletting or outsourcing shall be done and the project shall only be executed by the Bidder. An undertaking to be provided as per the template annexed (Refer Annexure F3) .
8.	The bidder shall follow the latest versions of frameworks and databases like OWASP, CVE, CVSS, CWSS and other industry standards for analyzing the security posture and the report which shall be provided to the Bank shall conform to the above-mentioned frameworks/databases.		Bidder to provide the undertaking on bidder's letter head duly signed by the Authorized signatory to confirm that the security assessment and the reports submitted by the bidder upon successful completion of the project will conform to the stated framework/databases. The report shall not be the raw reports exported/extracted from the tool and shall be reviewed manually to eliminate false positive observations. An undertaking to be provided as per the template annexed (Refer Annexure F3) .
9.	Bidders should have reported net profit for the last three financial years (2023-2024, 2022-2023 & 2021-2022)		Copy of audited balance sheet to be provided by the Bidder
10.	The manpower proposed to be engaged for the Comprehensive Security Review of the Bank (SBI Singapore) must be a domain expert with relevant certifications in Network Security, Database &		Bidder to provide the details (Count of resources, Name of Employee, Professional Experience in years, Certification) as annexure in a tabular format

Sr. No.	Eligibility Criteria	Compliance Y / N	Documents to be submitted
	Application Security, Cyber Forensics, DAST/SAST/IAST		

Note: Bidders to fill the above provided template and enclose all the undertakings and documents along with the template while submitting their proposals.

Annexure-C**Technical Evaluation Parameters:**

Detailed technical evaluation will include, scrutiny of minimum eligibility criteria (as mentioned in the RFP) and technical information submitted duly signed by authorized signatory all required supporting documents.

The Technical Proposal will be evaluated on the basis of Applicant's experience, its understanding of Scope of Work, proposed methodology and Work Plan, and the experience of Key Personnel. The following evaluation matrix will be used for technical evaluation.

S No	Evaluation Matrix	Yes/No	Mention the details as applicable (in Years/ No of Certified Officials)	Provide Details as per Annexure
1	Bidder's Years of Experience in the field of IT & Cyber Security Services is more than 3 years			F1
2	The bidder has executed at least 2 Comprehensive Security Reviews/ Similar Scale projects during the last 24 months			F2
3	The bidder has at least 10 accredited/certified personnel employed in the company. Note: Refer Point No 6 in the 'Eligibility Criteria' Section for the list of acceptable certificates.			Bidder to provide the details (Name of Employee, Professional Experience in years, Certification) as annexure in a tabular format
4	Out of the total number of certified personnel employed by the bidder, the bidder shall allocate 3 resources for this engagement and ensure timely completion of Comprehensive Security Review of SBI Singapore.			Bidder to provide the details (Name of Employee, Professional Experience in years, Certification) as annexure in a tabular format

Annexure-D

Pre-Bid Query Format
(To be provide strictly in Excel format)

Vendor Name	Sl. No	RFP Page No	RFP Clause No.	Existing Clause	Query/Suggestions

Annexure-E

NON-DISCLOSURE AGREEMENT

THIS RECIPROCAL NON-DISCLOSURE AGREEMENT (the “Agreement”) is made at _____ between:

State Bank of India Singapore, which is a part of State Bank of India, constituted under the State Bank of India Act, 1955 having its Corporate Centre and Central Office at State Bank Bhavan, Madame Cama Road, Nariman Point, Mumbai-21 through its Risk Management Department at 80 Robinson Road, Singapore (hereinafter referred to as “Bank” which expression includes its successors and assigns) of the ONE PART;

And

_____ a private/public limited company/LLP/Firm ~~<strike off whichever is not applicable>~~ incorporated under the provisions of the Companies Act ~~<strike off whichever is not applicable>~~, having its registered office at _____ (hereinafter referred to as “_____” which expression shall unless repugnant to the subject or context thereof, shall mean and include its successors and permitted assigns) of the OTHER PART;

And Whereas

1. _____ is carrying on business of providing _____, has agreed to _____ for the Bank and other related tasks.

2. For purposes of advancing their business relationship, the parties would need to disclose certain valuable confidential information to each other (the Party receiving the information being referred to as the “Receiving Party” and the Party disclosing the information being referred to as the “Disclosing Party. Therefore, in consideration of covenants and agreements contained herein for the mutual disclosure of confidential information to each other, and intending to be legally bound, the parties agree to terms and conditions as set out hereunder.

NOW IT IS HEREBY AGREED BY AND BETWEEN THE PARTIES AS UNDER

1. **Confidential Information and Confidential Materials:**

- (a) “Confidential Information” means non-public information that Disclosing Party designates as being confidential or which, under the circumstances surrounding disclosure ought to be treated as confidential. “Confidential Information” includes, without limitation, information relating to developed, installed or purchased Disclosing Party software or hardware products, the information relating to general architecture of Disclosing Party’s network, information relating to nature and content of data stored within network or in any other storage media, Disclosing Party’s business policies, practices, methodology, policy design delivery, and information received from others that Disclosing Party is obligated to treat as confidential. Confidential Information disclosed to Receiving Party by any Disclosing Party Subsidiary and/ or agents is covered by this agreement
- (b) Confidential Information shall not include any information that: (i) is or subsequently becomes publicly available without Receiving Party’s breach of any obligation owed to Disclosing party; (ii) becomes known to Receiving Party free from any confidentiality obligations prior to Disclosing Party’s disclosure of such information to Receiving Party; (iii) became known to Receiving Party from a source other than Disclosing Party other than by the breach of an obligation of confidentiality owed to Disclosing Party and without confidentiality restrictions on use and disclosure; or (iv) is independently developed by Receiving Party.
- (c) “Confidential Materials” shall mean all tangible materials containing Confidential Information, including without limitation written or printed documents and computer disks or tapes, whether machine or user readable.

2. **Restrictions**

- (a) Each party shall treat as confidential the Contract and any and all information (“confidential information”) obtained from the other pursuant to the Contract and shall not divulge such information to any person (except to such party’s “Covered Person” which term shall mean employees, contingent workers and professional advisers of a party who need to know the same) without the other party’s written consent provided that this clause shall not extend to information which was rightfully in the possession of such party prior to the commencement of the negotiations leading to the Contract, which is already public knowledge or becomes so at a future date (otherwise than as a result of a breach of this clause). Receiving Party will have executed or shall execute appropriate written agreements with Covered Person, sufficient to

enable it to comply with all the provisions of this Agreement. If Service Provider appoints any Sub-Contractor (if allowed) then Service Provider may disclose confidential information to such Sub-Contractor subject to such Sub Contractor giving the Bank an undertaking in similar terms to the provisions of this clause. Any breach of this Agreement by Receiving Party's Covered Person or Sub-Contractor shall also be constructed a breach of this Agreement by Receiving Party.

- (b) Receiving Party may disclose Confidential Information in accordance with judicial or other governmental order to the intended recipients (as detailed in this clause), provided Receiving Party shall give Disclosing Party reasonable notice (provided not restricted by applicable laws) prior to such disclosure and shall comply with any applicable protective order or equivalent. The intended recipients for this purpose are:
 - i. the statutory auditors of the either party and
 - ii. government or regulatory authorities regulating the affairs of the parties and inspectors and supervisory bodies thereof
- (c) Confidential Information and Confidential Material may be disclosed, reproduced, summarized or distributed only in pursuance of Receiving Party's business relationship with Disclosing Party, and only as otherwise provided hereunder. Receiving Party agrees to segregate all such Confidential Material from the confidential material of others in order to prevent mixing.

3. **Rights and Remedies**

- (a) Receiving Party shall notify Disclosing Party immediately upon discovery of any unauthorized used or disclosure of Confidential Information and/ or Confidential Materials, or any other breach of this Agreement by Receiving Party, and will cooperate with Disclosing Party in every reasonable way to help Disclosing Party regain possession of the Confidential Information and/ or Confidential Materials and prevent its further unauthorized use.
- (b) Receiving Party shall return all originals, copies, reproductions and summaries of Confidential Information or Confidential Materials at Disclosing Party's request, or at Disclosing Party's option, certify destruction of the same.
- (c) Receiving Party acknowledges that monetary damages may not be the only and / or a sufficient remedy for unauthorized disclosure of Confidential Information and that disclosing party shall be entitled, without waiving any other rights or remedies (including but not limited to as listed below), to

injunctive or equitable relief as may be deemed proper by a Court of competent jurisdiction.

- i. Suspension of access privileges
 - ii. Change of personnel assigned to the job
 - iii. Termination of contract
- (d) Disclosing Party may visit Receiving Party's premises, with reasonable prior notice and during normal business hours, to review Receiving Party's compliance with the term of this Agreement.

4. **Miscellaneous**

- (a) All Confidential Information and Confidential Materials are and shall remain the sole and of Disclosing Party. By disclosing information to Receiving Party, Disclosing Party does not grant any expressed or implied right to Receiving Party to disclose information under the Disclosing Party's patents, copyrights, trademarks, or trade secret information.
- (b) Confidential Information made available is provided "As Is," and disclosing party disclaims all representations, conditions and warranties, express or implied, including, without limitation, representations, conditions or warranties of accuracy, completeness, performance, fitness for a particular purpose, satisfactory quality and merchantability provided same shall not be construed to include fraud or willful default of disclosing party.
- (c) Neither party grants to the other party any license, by implication or otherwise, to use the Confidential Information, other than for the limited purpose of evaluating or advancing a business relationship between the parties, or any license rights whatsoever in any patent, copyright or other intellectual property rights pertaining to the Confidential Information.
- (d) The terms of Confidentiality under this Agreement shall not be construed to limit either party's right to independently develop or acquire product without use of the other party's Confidential Information. Further, either party shall be free to use for any purpose the residuals resulting from access to or work with such Confidential Information, provided that such party shall maintain the confidentiality of the Confidential Information as provided herein. The term "residuals" means information in non-tangible form, which may be retained by person who has had access to the Confidential Information, including ideas, concepts, know-how or techniques contained therein. Neither party shall have any obligation to limit or restrict the assignment of such persons or to pay royalties for any work resulting from the use of

residuals. However, the foregoing shall not be deemed to grant to either party a license under the other party's copyrights or patents.

- (e) This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof. It shall not be modified except by a written agreement dated subsequently to the date of this Agreement and signed by both parties. None of the provisions of this Agreement shall be deemed to have been waived by any act or acquiescence on the part of Disclosing Party, its agents, or employees, except by an instrument in writing signed by an authorized officer of Disclosing Party. No waiver of any provision of this Agreement shall constitute a waiver of any other provision(s) or of the same provision on another occasion.
- (f) In case of any dispute, both the parties agree for neutral third-party arbitration. Such arbitrator will be jointly selected by the two parties and he/she may be an auditor, lawyer, consultant or any other person of trust. The said proceedings shall be conducted in English language at Mumbai and in accordance with the provisions of Singapore Laws. Nothing in this clause prevents a party from having recourse to a court of competent jurisdiction for the sole purpose of seeking a preliminary injunction or any other provisional judicial relief it considers necessary to avoid irreparable damage. This Agreement shall be governed by and construed in accordance with the laws of Republic of India. Each Party hereby irrevocably submits to the exclusive jurisdiction of the courts of Mumbai.
- (g) Subject to the limitations set forth in this Agreement, this Agreement will inure to the benefit of and be binding upon the parties, their successors and assigns.
- (h) If any provision of this Agreement shall be held by a court of competent jurisdiction to be illegal, invalid or unenforceable, the remaining provisions shall remain in full force and effect.
- (i) The Agreement shall be effective from _____ ("Effective Date") and shall be valid for a period of _____ year(s) thereafter (the "Agreement Term"). The foregoing obligations as to confidentiality shall survive the term of this Agreement and for a period of five (5) years thereafter provided confidentiality obligations with respect to individually identifiable information, customer's data of Parties or software in human-readable form (e.g., source code) shall survive in perpetuity.

5. **Suggestions and Feedback**

Either party from time to time may provide suggestions, comments or other feedback to the other party with respect to Confidential Information provided

originally by the other party (hereinafter “feedback”). Both parties agree that all Feedback is and shall be entirely voluntary and shall not in absence of separate agreement, create any confidentially obligation for the receiving party. However, the Receiving Party shall not disclose the source of any feedback without the providing party’s consent. Feedback shall be clearly designated as such and, except as otherwise provided herein, each party shall be free to disclose and use such Feedback as it sees fit, entirely without obligation of any kind to other party. The foregoing shall not, however, affect either party’s obligations hereunder with respect to Confidential Information of other party.

Dated this _____ day of _____ (Month) 20__ at _____(place)

For and on behalf of _____

Name		
Designation		
Place		
Signature		

For and on behalf of _____

Name		
Designation		
Place		
Signature		

Annexure- F1

Bidder Details

Details of the Bidder

S. No.	Particulars	Details
1.	Name	
2.	Date of Incorporation and / or commencement of business	
3.	Certificate of incorporation	
4.	Brief description of the Bidder including details of its main line of business	
5.	Company website URL	
6.	Company ACRA Number	
7.	Particulars of the Authorized Signatory of the Bidder a) Name b) Designation c) Address d) Phone Number (Landline) e) Mobile Number f) Fax Number g) Email Address	

(Signature)

(Name)

(In the capacity of)

Duly authorized to sign Bid for and on behalf of

Seal of the company.

Annexure- F2

Engagement of the bidder's organization in the Financial Industry sector in context with the scope of work –Security Review

For the period April 2022 to March 2024

Sl. No.	Name of the organisation engaged where	Nature of work (Detailed Description)	Date of Purchase order (2020-23)	Supporting documents (Enclosed /Not Enclosed)
1				
2				
3				

Please Note:

Supporting documents for above should be Purchase / Work Orders, letters from clients on their letter head, contacts of clients etc.

(Signature)

(Name)

(In the capacity of)

Duly authorized to sign Bid for and on behalf of

Seal of the company.

**Undertaking by Bidder
(To be provided on the Bidder's Letterhead)**

Date:

To,
Chief Executive Officer
State Bank of India,
27-01, 80 Robinson Road,
Singapore, 068898

Subject: Undertaking for Compliance with Terms and Conditions of the Bid

We, M/s [Insert Bidder's Name], having our registered office at [Insert Address], hereby submit this undertaking in relation to the tender/bid [Insert Tender Reference Number and Description].

We solemnly affirm and undertake the following:

a) Non-Usage of Open Source or Cloud-Based Solutions:

We confirm that no open-source or cloud-based solutions will be used in the execution of this contract unless explicitly authorized in writing by [Insert Organization Name].

b) No Existing Litigation:

We hereby declare that no litigation or arbitration proceedings exist against our firm that could adversely affect our ability to perform the obligations of this contract.

c) No Corruption or Ineligibility:

We confirm that neither our firm nor any of its directors, partners, or stakeholders have been charged with corruption, nor has our firm been declared ineligible or blacklisted by any government or regulatory authority in India or abroad.

d) No Subletting of Work:

We undertake that no portion of the awarded work shall be sublet to any third party, and the work will be carried out solely by us.

e) Adherence to Latest Security Frameworks:

We confirm that we shall comply with the latest security frameworks and best practices, including but not limited to: - Common Vulnerability Scoring System (CVSS), Open Web Application Security Project (OWASP).

f) Compliance with All Applicable Laws and Regulations:

We undertake to abide by all applicable laws, rules, and regulations governing the execution of the contract. We fully understand that any violation of the above terms may lead to immediate termination of the contract and other actions as deemed necessary by the Bank.

(Signature)

(Name)

(In the capacity of)

Duly authorized to sign Bid for and on behalf of

Seal of the company.

Annexure-G

Commercial Bid

The indicative Price Bid needs to contain the information listed hereunder and needs to be submitted on portal of e-Procurement agency.

Sl. No.	Project Details	Total Cost
1	Commercial Bid for Comprehensive Security Review of Applications as per the Scope defined in this RFP Document.	
	Total	

(Amount quoted in SGD exclusive of GST)

Dated this day of 2024

(Signature)

(Name)

(In the capacity of)

Duly authorized to sign Bid for and on behalf of

Seal of the company.