Request for Proposal (RFP)

For Empanelment of

Information Security Service Providers (ISSPs)

State Bank Global IT Centre
Information Security Department
'A'- Wing, Ground Floor
Sector 11, CBD Belapur
Navi Mumbai 400614
INDIA

Document	**Empanelment of Information Security Service Providers (ISSP) for 2024-27**
RFP No.	**SBI/GITC/ISD/2023-24/ISO/43**
Date	**31.03.2024**
Contact	**Shri Vijay Kumar, Asstt. General Manager (Admin)**

Schedule of Events

Sl No	Particulars	Remarks
1	Contact details of issuing department (Name, Designation, Mobile No. Email address for sending any kind of correspondence regarding this RFP)	Shri Mukesh Kumar, CM (Admin) admin.isd@sbi.co.in Mobile No.: 9826340219 mail copy to be marked to Shri Vijay Kumar, Asst General Manager (Admin) Email: agm2.isd@sbi.co.in Mobile No.: 7880474316
2	Last date for requesting clarification	**Up to 05.30 PM on 30.04.2024** All communications regarding points / queries requiring clarifications shall be given in writing or by e-mail.
3	Pre - bid meeting or responses by the Bank	By 05.00 P.M. on 03.05.2024
4	Last date and time for Bid submission	**Up to 4.00 P.M. on 13.05.2024**
5	Address for submission of Bids (Online submission)	*https://etender.sbi/SBI*
6	Date and Time of opening of Technical Bids	11.30 AM on 15.05.2024. Authorized representatives of Bidders may be present online during the opening of the Technical Bids. However, Technical Bids would be opened even in the absence of any or all of Bidders representatives.
7	Tentative date of virtual Presentation by bidders	Will be advised seperately
8	Reverse Auction	On a subsequent date which will be communicated to such Bidders who qualify in the Technical Bid.
9	BID Validity from the date of BID submission	180 days
10	Contact details of e-Procurement agency appointed for e-procurement	**e-Procurement Technologies LTD – CMMI5** E-mail ID: nandan.v@eptl.in Landline No. : 079 6813 6820, 6850, 6857, 6848 Official Mobile No. : 9081000427 Ravi Sheladiya ravi.s@auctiontiger.net 07968136856

Part-I

Part-II

1. INVITATION TO BID:

State Bank of India (herein after referred to as **'SBI/the Bank')**, having its Corporate Centre at Mumbai, various other offices (LHOs/ Head Offices /Zonal Offices/Global Link Services, Global IT Centre, foreign offices etc.) of State Bank of India, branches/other offices, Subsidiaries and Joint Ventures available at various domestic and foreign locations and managed by the Bank (collectively referred to as **'State Bank Group'** or **'SBG'** or **'SBI'** hereinafter). This Request for Proposal (RFP) has been issued by the Bank**.**

This RFP seeks proposal from the CERT-In empaneled Information Security Auditing Organizations (bidders) to provide Information Security Services to SBI adhering to the Bank's requirement(s) outlined in this RFP. The criteria and the actual process of evaluation of the responses to this RFP and subsequent selection of the successful bidder(s) will be entirely at the Bank's discretion. The successful bidder(s) will continue to be in the panel of SBI to provide information security services as long as their CERT-In empanelment as above is in force.

This RFP is not an offer by State Bank of India, but an invitation to receive responses from the Bidders. No contractual obligation whatsoever shall arise from the RFP process unless and until a formal contract is signed and executed by duly authorized official(s) of State Bank of India with the selected Bidders.

i. Address for submission of online Bids, contact details including email address for sending communications are given in Schedule of Events of this RFP.
ii. The purpose of SBI behind this RFP is to seek a detailed technical proposal for empanelment of ISSPs for providing Information Security Services desired in this RFP.
iii. This RFP document shall not be transferred, reproduced, or otherwise used for purpose other than for which it is specifically issued by the bidders.
iv. The eligible Bidders desirous of providing proposed **S**ervice**s** to SBI are invited to submit their technical proposal in response to this RFP. The criteria and the actual process of evaluation of the responses to this RFP and subsequent selection of the successful Bidder will be entirely at Bank's discretion. These bidders must have necessary experience, capability & expertise to provide SBI the proposed **S**ervice**s** adhering to Bank's requirements outlined in this RFP.

2. DISCLAIMER:

i. The information contained in this RFP or information provided subsequently to Bidder(s) whether verbally or in documentary form/email by or on behalf of SBI, is subject to the terms and conditions set out in this RFP.
ii. This RFP is not an offer by State Bank of India, but an invitation to receive responses from the eligible Bidders.
iii. The purpose of this RFP is to provide the Bidder(s) with information to assist preparation of their Bid proposals. 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.

3. DEFINITIONS:

In this connection, the following terms shall be interpreted as indicated below:

i. **"The Bank"** 'means the State Bank of India (including domestic branches and foreign offices), domestic and foreign Subsidiaries and Joint Ventures, where the Bank has ownership of more than 50% of voting securities or the power to direct the management and policies of such Subsidiaries and Joint Ventures.

ii. **"Bidder/Channel Partner"** means an eligible entity/firm submitting the Bid in response to this RFP.

iii. **"Bid"** means the written reply or submission of response to this RFP.

iv. **"The Contract"** means the agreement entered into between the Bank and Service Provider, as recorded in the Contract Form signed by the parties, including all attachments and appendices thereto and all documents incorporated by reference therein.

v. **"Total Contract Price/Project Cost/TCO"** means the price payable to Service Provider over the entire period of Contract for the full and proper performance of its contractual obligations.

vi. **"Vendor/Service Provider"** is the successful Bidder found eligible as per eligibility criteria set out in this RFP, whose technical Bid has been accepted and who has emerged as L1 (lowest in reverse auction) Bidder as per the selection criteria set out in the RFP and to whom notification of award has been given by the Bank.

vii. **"ISSP"** Information Security Service Provider or Information Security Auditing Organizations empaneled with CERT-In.

viii. **"Services"** means all services, scope of work and deliverables to be provided by a Bidder as described in the RFP and include provision of technical assistance, training, certifications, auditing and other obligation of Service Provider covered under this RFP.

ix. **Annual Maintenance Contract (AMC)** - It would be the annual cost of maintenance/upkeep/up-dation of product or specified hardware and software.

4. SCOPE OF WORK:

Scope of work involves various security related task/assignments. Details are as given in Appendix–B.

5. EMPANELMENT PERIOD:

The empanelment of ISSPs is proposed to be for a period of 36 months or up to March 2027 (whichever is earlier). This would be subject to satisfactory performance and periodical review, as desired by the Bank from time to time. The Bank reserves the right to de-empanel any empaneled ISSP. Empanelment does not confer any rights on the bidders to necessarily receive assignments/jobs. The allocation of assignments/jobs will be at the sole discretion of the Bank.

6. ELIGIBILITY CRITERIA:

Bid is open to all CERT-In Empaneled Information Security Auditing Organizations/Bidders who fulfil the eligibility criteria. The bidder has to submit the details of eligibility criteria as per Annexure – B.

7. SKILL SET AND EXPERIENCE REQUIREMENTS OF RESOURCES:

Through this empanelment, the empaneled bidders are required to provide resources with the following skill set and experiences.

Level 1 Experience of 1 year and up to 4 years	**Educational qualifications:** Graduation in CS or IT or Information Security or Cyber Security • Minimum 2 of Mandatory Certifications: CEH/LPT/ISO 27001 LA/LI or Certifications. • Experience: Having good experience in application & Infrastructure security assignments. Have done IS assessments OR IS systems/solution management.
Level 2	

Experience of above 4 years and upto 8 years	**Educational qualifications:** Graduation in CS or IT or Information Security or Cyber Security • Mandatory certifications: CISA/CISM/CISSP/OSCP/ Infrastructure security solution certifications. • Experience: In carrying out security assessments. Excellent knowledge in security solutions and technologies. Banking domain knowledge will be added advantage.
Level 3 Experience of above 8 years and upto 12 years	**Educational qualifications:** Education Graduation in CS or IT or Information Security or Cyber Security • Mandatory certifications: CISA/CISM/CISSP/OSCP/ OSCE (Minimum two) / Infrastructure security solution certifications. • Experience: excellent domain knowledge in application or infrastructure management / assessments. Banking domain knowledge will be added advantage.
Level 4 Experience above 12 years	**Educational qualifications:** Graduation in CS or IT or Information Security or Cyber Security • Mandatory certifications: CISA and two of CISSP/OSCP/OSCE/CEH/ Infrastructure security solution certifications. • Experience: excellent domain knowledge in application or infrastructure management / assessments. Banking domain knowledge will be added advantage.

Subcontracting/hiring of external resources is not permitted.

8. BIDDING PROCESS:

It is mandatory for all the Bidders to have class-III Digital Signature Certificate (DSC) (in the name of person who will sign the Bid) from any of the licensed certifying agency to participate in this RFP. DSC should be in the name of the authorized signatory. It should be in corporate capacity (that is in Bidder capacity).

All details with the relevant information / documents / acceptance of all terms and conditions strictly as described in this RFP will have to be submitted. Only TECHNICAL BID will be opened and evaluated. Bidders satisfying eligibility criteria and agreeing to comply with all terms and conditions specified in this document will be evaluated for technical specifications. Those bids that have been shortlisted after evaluating the Technical bids shall be eligible to participate in the reverse auction.

9. PREPARATION AND SUBMISSION OF BIDS:

Bids prepared by the bidder and all correspondence and documents relating to bids exchanged by the bidder and purchaser must be written in English. Any non-English language responses should be accompanied by a certified English translation.
Bidder must provide individual and factual replies to specific questions asked in the RFP.

The Bidder must thoroughly study/analyze and properly understand the contents of this RFP, its meaning and impact of the information contained therein.

Failure to furnish all information required in this RFP or submission of Bid not responsive to this RFP in any respect will be at the Bidder's risk and responsibility and the same may finally result in rejection of its Bid. The Bank has made considerable effort to ensure that accurate information is contained in this RFP and is supplied solely as guidelines for Bidders.

The Bid prepared by the Bidder, as well as all correspondences and documents relating to the Bid exchanged by the Bidder and the Bank and supporting documents and printed literature shall be submitted in English.

The information provided by the Bidders in response to this RFP will become the property of the Bank and will not be returned. Incomplete information in Bid document may lead to non-consideration of the proposal.

Documents mentioned below are to be uploaded on portal of e-Procurement agency with digital signature of authorized signatory:

i. Technical Bid covering letter/Bid form on the lines of Appendix-A on Bidder's letter head.
ii. Bidder's information as per Annexure A on bidder's letter head.
iii. Bank may ask for word copy of all the technical evaluation formats (Annexure C1 to C10) from all interested ISSPs after opening of online technical bids.

iv. Audited balance sheets and profit and loss account statement for last 2 years
v. A copy of board resolution or power of attorney showing that the signatory has been duly authorized to sign the tender document.
vi. Response to all points of the technical evaluation format should be as per Annexure C, C1, C2, C3, C4, C5, C6, C7 & C8.
vii. Non-Disclosure Agreement as per Annexure D
viii. Compliance Statement as per Annexure E

10. PRE-BID MEETING:

SBI may, at its sole discretion, organize a pre-bid meeting in-person or online, to resolve any queries, bidders may have. Any further information will be provided to all bidders by email. ISSPs may submit their pre-bid queries as per Appendix-C by emails as per schedule of events.

11. EMPANELMENT PROCESS:

11.1 Preliminary Examination:

Bids will be examined by the Bank to determine whether they are complete. A bid determined as not substantially responsive will be rejected. The Bank may, at its discretion waive any minor non-conformity or irregularity in a bid which does not constitute a material deviation.

After opening of the technical bids and preliminary examinations, some or all the bidders may be asked to make presentation of the services offered by them.

Any effort on the part of bidder to influence bid evaluation process or award of contract may result in the rejection of the bid.

11.2 Technical Evaluation:

All the Bids will be opened at the date, time & locations mentioned under the clause Bid Details. The technical bids will be opened in the presence of representatives of the bidders who choose to attend through e-procurement agency's portal.

11.3 Opening of Technical Bid:

Detailed technical evaluation will include, scrutiny of minimum eligibility criteria (as mentioned in Annexure B) and technical information submitted as per technical bid format (Annexure C, C1, C2, C3, C4, C5, C6, C7 & C8), proposed services, presentation, reference calls and site visits, if required. The bidder may highlight the noteworthy / superior features of their services. The bidder will demonstrate/substantiate all claims made in the technical bid to the

satisfaction of the Bank, the capability of the services to support all the requirements at their cost in their lab / office / in any other organization where services are being provided.

The evaluation will also consider:

- State of the art services offered by the bidder to any noticeable Bank in India. The bidder should furnish the details when requested.
- Capability of the proposed services to meet future requirements not outlined in the RFP.
- In house development capability of tools / utilities.
- Bidder support facilities

11.4 Technical – Evaluation Parameter

#	Activities related to Information Security	Weightage %
1	Indian & Global clients' assignments handled	20
2	Skilled personnel resources available	15
3	Organisation Skill: Technical skills & Credentials (tools created, R&D work done, papers/journals published, forensics assignments done)	5
4	Depth & Breadth of information security assignments handled. Credentials / certifications etc. Committee membership in Govt / RBI /IDRBT / Cert-IN / Gartner etc.	30
5	Presentation to TPNC committee	20
6	Client feedback of two (2) clients of national/international repute as provided in point 1 in this table	10
	Total	**100**

Percentage Marks Scored…….

Technical Evaluation Excel sheet has also been shared along with this RFP for the information of the bidders. Bidders should fill in their credentials in the Technical evaluation sheet and share with the Bank as a part of technical bid. Bidders to note that, Tentative Score shown in the sheet based on the credentials filled in by the bidders shall not be final and binding on the Bank. The Bank's decision on score allotted to bidders as a part of technical evaluation thereof shall be final.

Bidders will be shortlisted on the basis of score allotted to them by the Bank based on technical evaluation & subsequent presentation made by them, shall be eligible to participate in the reverse auction.

Bidders scoring less than 80 % will not be considered for further evaluation.

However, Bank reserves right to evaluate periodically i.e., first evaluation will be on March 2025 and subsequently during March 2026, March 2027 (annually).

- Competency in IT, Information and Cyber Security areas in general, having good pool of L1, L2, L3 & L4 resources, for our project-based basis engagement. Generally, Bank requires 80 resources on daily basis with competency in AppSec, Code Review, VA, PT, SCD / Hardening Check, Secured Network Architecture (SNA) and Process Review etc. Experience and expertise in carrying out:-
- Security risk assessments of applications, API, Web, Database, Middleware.
- Security risk assessments of the Network architecture, design, Firewalls, IPS, Wi-Fi, VPN etc.
- Experience and expertise in Infrastructure & data security related areas of Active Directory, Email security, DNS, Proxy, Data security (DLP, DRM),
- Experience in implementing Information security projects as and when they come up.
- ISSPs will be offered Review/Consultancy related to niche areas of IT, Information and Cyber Security, including but not limited to complex architecture, New/Advanced IT technology, processes, evaluation of technologies, developing / reviewing of policies, procedures, strategies, plans etc.

Post empanelment, the allocation / distribution of activities / assignments will be solely at the discretion of the Bank, which will include calling bids from ISSPs for getting techno-commercial effort estimates and discovering L1 bidder through online reverse auction or sealed envelope mode.

Empanelment by the Bank does not confer any right on the bidder to receive assignments / activities / work orders from the Bank.

The Bank reserves the right to accept the bids or opt for negotiation and offer the rates or cancel the entire RFP process.

In case ISSPs performance is not found up to the mark during internal periodical review, they may be de-empaneled.

11.5 Commercial evaluation & finalization:

Sr. No.	Resource Level	Resource Cost per person /per day (Rs.)	Resource Cost per person / per month (Rs.) (if retained for a minimum duration of one month for a regular routine)
1.	L-1		
2.	**L-2**	**1.42 Times of L-1**	**1.42 Times of L-1**
3.	**L-3**	**1.73 Times of L-1**	**1.73 Times of L-1**
4	**L-4**	**2.55 Times of L-1**	**2.55 Times of L-1**
…			

The Commercial offers received on E-Tender portal of only those Bidders, who are short-listed after technical evaluation **(Technically Qualified)**, would be opened. The format for quoting commercial bid set out in Annexure F.
Commercial quotes received from the technically qualified Bidders will be opened and compared. **We will discover the price for L-1 resource level through reverse auction process and for L-2, L-3 & L-4 resource level pricing will be defined as per the multiplication factor mentioned in the above table.** The L-1 price discovered through reverse auction will be offered to the other technically qualified bidders. All the technically qualified bidders **(Maximum-15 Vendors will be empaneled)** accepting the L-1 price discovered through reverse auction will be empaneled at those rates.
Post empanelment, the allocation / distribution of activities / assignments will be solely at the discretion of the Bank, which will include calling RFP for getting effort estimates.
Empanelment by the Bank does not confer any right on the vendor to receive assignments / activities / work orders.
The Bank reserves the right to accept the bids or opt for negotiation and offer the rates or cancel the entire RFP process.

Post empanelment, all ISSPs as defined in 11.4 above. Bank has already discovered the base price for their personnel resources in various levels viz. L1, L2, L3 and L4. Base Price will be shared with Bidders Post empanelment. Depending on the engagement model and activity, eligible ISSPs will be invited for the commercial bids. Eligible ISSPs may quote premium or discount to the base price. The lowest quoted bidder through online reverse auction / sealed bid method will be awarded the assignment. There may be negotiations or reverse auction within the ISSPs.

12. SIGNING OF MASTER SERVICE LEVEL AGREEMENT (MSLA) FOR EMPANELMENT:

SBI will notify successful bidder(s) **(Maximum-15 ISSP Vendors will be empaneled)** in writing by letter in duplicate or email/ fax that its bid has been accepted. The Selected bidder(s) must return the duplicate copy to the Bank within 7 working days duly Accepted, Stamped and Signed by Authorized Signatory in token of acceptance.

The successful bidder(s) shall be required to enter into a contract/Master SLA with the Bank, within 7 days of intimation of empanelment or within such extended period as may be decided by the Bank along with the letter of acceptance, Non-Disclosure Agreement(NDA), BG and other terms and conditions as may be determined by the Bank to be necessary for the due performance of the work in accordance with the Bid and acceptance thereof.

Copy of board resolution or power of attorney showing that the signatory has been duly authorized to sign the acceptance letter, contract and NDA should be submitted.

In case of failure to accept the empanelment within 7days from the date of receipt of the communication, the Bank will be at liberty to cancel/drop the empanelment offer for that vendor.

The contract/agreement will be based on bidder's offer document with all its enclosures, modifications arising out of negotiation /clarifications etc., and will include SLA, project plan – phases & milestones and schedule, copies of all necessary documents, licenses, certifications etc.

The Bank reserves the right to stipulate, at the time of finalization of the contract, that any other document(s) to be enclosed as a part of the final contract.

13. MODEL OF ENGAGEMENT WITH THE EMPANELLED BIDDERS

The empanelment is for 36 months from date of signing of SLA with the Bank or up to March 2027 (whichever is earlier). The services of Vendors empaneled through this RFP will be engaged at SBI and other companies as and when requirements arise as per following models.

13.1 Price model:
For an assignment / project / task (viz., Comprehensive Security Review of Applications / Preparation of policy document / Forensic Audit etc.) the Bank will call for RFP from multiple empaneled t. The vendors have to quote the prices considering the efforts involved. The lowest quoted vendor will be awarded the assignment. There may be negotiations or reverse auction within the invited ISSPs.

13.2 Project based model:
The vendors have to quote the prices considering the efforts involved. The lowest quoted vendor will be awarded the assignment. There may be negotiations or reverse auction within the ISSPs.

13.3 Nomination model:
For special projects or on emergency basis, the Bank may assign the project on nomination and negotiation basis.

Even though the empanelment is for 36 months or up to March 2027 (whichever is earlier), periodical performance review of selected bidder will be carried out by the Bank. Depending on the performance review, the selected bidder may be continued or may be de-empaneled.

Decision of the Bank is final in awarding the assignment / contract depending on a project suitable engagement model.

14. SPECIFIC TERMS & CONDITIONS:

14.1 Format and Signing of Bid
Technical Bid covering letter/Bid form on the lines of Appendix-A on Bidder's letter head.

The Technical Bid is to be submitted on portal of e-Procurement agency for Request For Proposal (RFP) For Empanelment of Information Security Service Providers (ISSPs) RFP No. SBI/GITC/ISD/2023-24/ISO/43 dated 31-03-2024. Documents mentioned below have to be uploaded on portal of e-Procurement agency with digital signature of authorized signatory of the bidders.

All pages of the Bid document should be serially numbered and shall be digitally signed by the authorized signatory / signatories only. The bidder should submit a copy of board resolution or power of attorney showing that each signatory has been duly authorized to sign the tender document.

Any interlineations, erasures or overwriting shall be valid only if the person(s) signing the bid sign(s) them.

In case of any discrepancies between hard and soft copy, the hard copy will be considered as base document.

Bidders may please note below w.r.t. this RFP process:

(a) The Bidder should quote for the entire package on a single responsibility basis for Services it proposes to supply.
(b) While submitting the Technical Bid, literature on the Services should be segregated and kept together in one section.
(c) Care should be taken that the Technical Bid shall not contain any price information. Such proposal, if received, will be rejected.

(d) The Bid document shall be complete in accordance with various clauses of the RFP document or any addenda/corrigenda or clarifications issued in connection thereto, submitted by the authorized representative of the Bidder.
(e) It is mandatory for all the Bidders to have class-II/III Digital Signature Certificate (DSC) (in the name of person who will sign the Bid) from any of the licensed certifying agency to participate in this RFP. DSC should be in the name of the authorized signatory. It should be in corporate capacity (that is in Bidder capacity).
(f) Bids are liable to be rejected if only one Bid (i.e. Technical Bid) is received.
(g) If deemed necessary, the Bank may seek clarifications on any aspect from the Bidder. However, that would not entitle the Bidder to change or cause any change in the substances of the Bid already submitted or the price quoted.
(h) The Bidder may also be asked to give presentation for the purpose of clarification of the Bid.
(i) The Bidder must provide specific and factual replies to the points raised in the RFP.
(j) The Bid shall be typed or written in indelible ink and shall be submitted by the Bidder or a person or persons duly authorized to bind the Bidder to the Contract.
(k) All the enclosures (Bid submission) shall be serially numbered. The person or persons signing the Bids shall initial all pages of the Bid.
(l) Any inter-lineation, erasures or overwriting shall be valid only if they are initialed by the person(s) signing the Bid.
(m)The Bank reserves the right to reject Bids not conforming to above.

14.2 Last date of receipt of bids

The bid should be submitted through e-procurement portal on or before last date as per Schedule of Events. The bank may at its discretion amend/extend the bid submission date. The modified target date & time will be notified to bidders through email.

14.3 Subcontracting

Subcontracting of any services is prohibited. If required in exceptional situations, Bidder has to obtain written permission from the Bank before contracting any work to subcontractors. Bank at its own discretion may permit or deny the same.

In case of subcontracting permitted, the contracting vendor is responsible for all the services provided to the Bank regardless of which entity is conducting the operations. The contracting vendor is also responsible for ensuring that the sub-contractor comply with all security requirements of the contract and Bank can obtain independent audit report for the same.

The bidder should provide subcontracting details to the Bank and if required, Bank may evaluate the same.

14.4 Cancellation of Contract

This RFP seeks proposal from the CERT-In empaneled entities to provide Information Security Services to SBI adhering to the Bank's requirement(s) outlined in this RFP. The successful bidder(s) will continue to be in the panel of

SBI to provide information security services if their CERT-In empanelment is in force. The moment, they are de-empaneled from the Empanelment List of CERT-In, for reasons whatsoever, they would stand de-empaneled from SBI panel also. However, during the currency of this empanelment, if the de-empaneled bidder once again gets re-empaneled by Cert-In, such bidder will be re-empaneled, subject to annual review by the Bank.

The Bank shall have the right to cancel the contract with the selected bidder at any time during the contract period, by giving a written notice of at least 3 (three) months, for any valid reason, including but not limited to the following:

i) Laxity in following security standards laid down by the Bank
ii) Excessive delay in execution of orders placed by the Bank
iii) Discrepancies / deviations in the agreed processes and/or products
iv) Violation of terms & conditions stipulated in this RFP
v) Non-participation in Bank projects by the selected bidder either by non-submission of the bid or after placement of Purchase Order by the Bank within the stipulated period.

If the performance of the empaneled ISSP is not satisfactory in an assignment awarded to them, the Bank may terminate the assignment and impose penalty for the same. The penalty may extend up to the contracted amount.

In the event of SBI terminating the Contract in whole or in part, SBI may assign, upon such terms and in such manner, as it deems appropriate, ISSP shall be liable to the Bank for excess costs for such similar services and services those are undelivered.

Bank reserves the right to report any misconduct on part of the selected bidder during empanelment or non-reporting of any material observation having impact on SBI reputation or threat to Information owned and held with SBI or non-following the clauses of this RFP and future agreement/SLA to be signed with SBI to RBI, SEBI, Cert-in, NCIIPC etc. or notify it publicly.

Bank also reserves its right to blacklist the defaulting bidder on temporary or permanent basis as also to de-empanel them.

14.5 Use of Tools:
The Empaneled bidders should use only licensed tools while performing various types of security reviews like AppSec, Code Review, VA, PT, SNA, Digital Forensic Analysis etc.

14.6 Deployment of resources:
The Empaneled bidders should deploy resources for review activities on ‘Project based Hire Model’ strictly as per Skill-set and educational/professional criteria as per para 7 of this RFP. In case the bidder fails to deploy as above, entire contract/assignment will be cancelled.

14.7 Active participation in bidding process:

The empaneled bidders should participate in all the RFP/Bidding process for allotment of jobs as per para 13 of this RFP. In case of non-participation, such bidders will be de-empaneled during their respective periodic review.

14.8 Responsibilities of the bidders:

The empaneled bidders, while providing Information Security Services to the Bank, are expected to provide qualitative and substantive report containing all vulnerabilities in an Application/IT Infrastructure. In case any compromise of data/information/Information Asset etc. surfaces on account of weakness/vulnerability in the particular Application/IT Infrastructure of which security review was done by the ISSP(s), the Bank reserves the right to blacklist the defaulting bidder on temporary or permanent basis as also to de-empanel the ISSP.

14.9 Place of assignments:

The bidders selected for empanelment and assigned the jobs as per para 13 of this RFP, need to deploy the personnel resources generally at offices of the Bank at Navi Mumbai and Mumbai cities. In a few cases, personnel resources may be required to deploy other cities in India or abroad for Information Security related services as per requirements.

In case of on-site assignments within the Mumbai and Navi Mumbai region, no conveyance and out of pocket expenses shall be paid by the Bank. However, for the on-site assignments at the places, outside the Mumbai and Navi Mumbai region, the personnel resources will be eligible for transportation and out of pocket expenses, in line with Master SLA agreed with existing empaneled ISSPs.

15. COST OF BID DOCUMENT:

The participating Bidders shall bear all the costs associated with or relating to the preparation and submission of their Bids including but not limited to preparation, copying, postage, delivery fees, expenses associated with any demonstration or presentations which may be required by the Bank or any other costs incurred in connection with or relating to their Bid. The Bank shall not be liable in any manner whatsoever for the same or for any other costs or other expenses incurred by a Bidder regardless of the conduct or outcome of the bidding process.

16. CLARIFICATION AND AMENDMENTS ON RFP/PRE-BID MEETING:

i. Bidder requiring any clarification on RFP may notify the Bank in writing strictly as per the format given in **Appendix-C** at the address/by e-mail within the date/time mentioned in the Schedule of Events.
ii. A pre-Bid meeting will be held in person or online on the date and time specified in the Schedule of Events which may be attended by the authorized representatives of the Bidders interested to respond to this RFP.
iii. The queries received (without identifying source of query) and response of the Bank thereof will be posted on the Bank's website or conveyed to the Bidders.
iv. The Bank reserves the right to amend, rescind or reissue the RFP, at any time prior to the deadline for submission of Bids. The Bank, for any reason, whether, on its own initiative or in response to a clarification requested by a

prospective Bidder, may modify the RFP, by amendment which will be made available to the Bidders by way of corrigendum/addendum. The interested parties/Bidders are advised to check the Bank's website regularly till the date of submission of Bid document specified in the Schedule of Events/email and ensure that clarifications / amendments issued by the Bank, if any, have been taken into consideration before submitting the Bid. Such amendments/clarifications, if any, issued by the Bank will be binding on the participating Bidders. Bank will not take any responsibility for any such omissions by the Bidder. The Bank, at its own discretion, may extend the deadline for submission of Bids in order to allow prospective Bidders a reasonable time to prepare the Bid, for taking the amendment into account. Nothing in this RFP or any addenda/corrigenda or clarifications issued in connection thereto is intended to relieve Bidders from forming their own opinions and conclusions in respect of the matters addresses in this RFP or any addenda/corrigenda or clarifications issued in connection thereto.

v. No request for change in commercial/legal terms and conditions, other than what has been mentioned in this RFP or any addenda/corrigenda or clarifications issued in connection thereto, will be entertained and queries in this regard, therefore will not be entertained.
vi. Queries received after the scheduled date and time will not be responded/acted upon.

17. MODIFICATION AND WITHDRAWAL OF BIDS:

i. The Bidder may modify or withdraw its Bid after the Bid's submission, provided that written notice of the modification, including substitution or withdrawal of the Bids, is received by the Bank, prior to the deadline prescribed for submission of Bids.
ii. A withdrawal notice may also be sent by the authorised representatives of the company through email, but followed by a signed confirmation copy, not later than the deadline for submission of Bids.
iii. No modification in the Bid shall be allowed, after the deadline for submission of Bids.
iv. No Bid shall be withdrawn in the interval between the deadline for submission of Bids and the expiration of the period of Bid validity specified in this RFP.
v. Withdrawn Bids, if any, will be returned unopened to the Bidders.

18. PERIOD OF BID VALIDITY AND VALIDITY OF PRICE QUOTED IN REVERSE AUCTION (RA):

i. Bid shall remain valid for duration of 6 calendar months from Bid submission date.
ii. Price quoted by the Bidder in Reverse auction shall remain valid for duration of 6 calendar months from the date of conclusion of RA.
iii. In exceptional circumstances, the Bank may solicit the Bidders' consent to an extension of the period of validity. The request and the responses thereto shall be made in writing. A Bidder is free to refuse the request. However, any extension of validity of Bids or price will not entitle the Bidder to revise/modify the Bid document.
iv. Once Purchase Order or Letter of Intent is issued by the Bank, the said

price will remain fixed for the entire Contract period and shall not be subjected to variation on any account, including exchange rate fluctuations and custom duty. A Bid submitted with an adjustable price quotation will be treated as non-responsive and will be rejected.

19. BID INTEGRITY:

Willful misrepresentation of any fact within the Bid will lead to the cancellation of the contract without prejudice to other actions that the Bank may take. All the submissions, including any accompanying documents, will become property of the Bank. The Bidders shall be deemed to license, and grant all rights to the Bank, to reproduce the whole or any portion of their Bid document for the purpose of evaluation and to disclose the contents of submission for regulatory and legal requirements.

20. CONTACTING THE BANK:

i. No Bidder shall contact the Bank on any matter relating to its Bid, from the time of opening of Technical Bid to the time, the Contract is awarded.
ii. 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 Bid.

21. POWERS TO VARY OR OMIT WORK:

i. No alterations, amendments, omissions, additions, suspensions or variations of the work (hereinafter referred to as variation) under the contract shall be made by the successful Bidder except as directed in writing by Bank. The Bank shall have full powers, subject to the provision herein after contained, from time to time during the execution of the contract, by notice in writing to instruct the successful Bidder to make any variation without prejudice to the contract. The finally selected Bidder shall carry out such variation and be bound by the same conditions as far as applicable as though the said variations occurred in the contract documents. If any, suggested variations would, in the opinion of the finally selected Bidder, if carried out, prevent him from fulfilling any of his obligations under the contract, he shall notify Bank thereof in writing with reasons for holding such opinion and Bank shall instruct the successful Bidder to make such other modified variation without prejudice to the contract. The finally selected Bidder shall carry out such variation and be bound by the same conditions as far as applicable as though the said variations occurred in the contract documents. If the Bank confirms its instructions, the successful Bidder's obligations shall be modified to such an extent as may be mutually agreed, if such variation involves extra cost. Any agreed difference in cost occasioned by such variation shall be added to or deducted from the contract price.
ii. In any case in which the successful Bidder has received instructions from the Bank as to the requirements for carrying out the altered or additional substituted work which either then or later on, will in the opinion of the finally selected Bidders, involve a claim for additional payments, such additional payments shall be mutually agreed in line with the terms and conditions of the order.
iii. If any change in the work is likely to result in reduction in cost, the parties

shall agree in writing so as to the extent of change in contract price, before the finally selected Bidder(s) proceeds with the change.

22. WAIVER OF RIGHTS:

Each Party agrees that any delay or omission on the part of the other Party to exercise any right, power or remedy under this RFP will not automatically operate as a waiver of such right, power or remedy or any other right, power or remedy and no waiver will be effective unless it is in writing and signed by the waiving Party. Further the waiver or the single or partial exercise of any right, power or remedy by either Party hereunder on one occasion will not be construed as a bar to a waiver of any successive or other right, power or remedy on any other occasion.

23. CONTRACT AMENDMENT:

No variation in or modification of the terms of the Contract shall be made, except by written amendment, signed by the parties.

24. BANK'S RIGHT TO ACCEPT ANY BID AND TO REJECT ANY OR ALL BIDS:

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 as specified in Award Criteria and Award of Contract, 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.

25. RIGHT TO VERIFICATION:

The Bank reserves the right to verify any or all of the statements made by the Bidder in the Bid document and to inspect the Bidder's facility, if necessary, to establish to its satisfaction about the Bidder's capacity/capabilities to perform the job.

26. RIGHT TO AUDIT:

i. The Selected Bidder (ISSP) shall be subjected to annual audit by internal/ external Auditors appointed by the Bank/ inspecting official from the Reserve Bank of India or any regulatory authority, covering the risk parameters finalized by the Bank/ such auditors in the areas of products (IT hardware/ Software) and services etc. provided to the Bank and Service Provider is required to submit such certification by such Auditors to the Bank. Service Provider and or his / their outsourced agents / sub – contractors (if allowed by the Bank) shall facilitate the same The Bank can make its expert assessment on the efficiency and effectiveness of the security, control, risk management, governance system and process created by Service Provider. Service Provider shall, whenever required by the Auditors, furnish all relevant information, records/data to them. All costs for such audit shall be borne by the Bank. Except for the audit done by Reserve Bank of India or any statutory/regulatory authority, the Bank shall provide reasonable notice not less than 7 (seven) days to Service Provider before such audit and same shall be conducted during normal business hours.

ii. Where any deficiency has been observed during audit of Service Provider

on the risk parameters finalized by the Bank or in the certification submitted by the Auditors, Service Provider shall correct/resolve the same at the earliest and shall provide all necessary documents related to resolution thereof and the auditor shall further certify in respect of resolution of the deficiencies. The resolution provided by Service Provider shall require to be certified by the Auditors covering the respective risk parameters against which such deficiencies have been observed.

iii. Service Provider further agrees that whenever required by the Bank, it will furnish all relevant information, records/data to such auditors and/or inspecting officials of the Bank/Reserve Bank of India and/or any regulatory authority(ies). The Bank reserves the right to call for and/or retain any relevant information /audit reports on financial and security review with their findings undertaken by Service Provider. However, Service Provider shall not be obligated to provide records/data not related to Services under the Agreement (e.g. internal cost breakup etc.).

27. LIMITATION OF LIABILITY:

i. The maximum aggregate liability of Service Provider, subject to clause *31 (iii)*, in respect of any claims, losses, costs or damages arising out of or in connection with this RFP/Agreement shall not exceed the total Project Cost.
ii. Under no circumstances shall either Party be liable for any indirect, consequential or incidental losses, damages or claims including loss of profit, loss of business or revenue.
iii. The limitations set forth herein shall not apply with respect to:

(a) claims that are the subject of indemnification pursuant to infringement of third-party Intellectual Property Right;
(b) damage(s) occasioned by the Gross Negligence or Willful Misconduct of Service Provider,
(c) damage(s) occasioned by Service Provider for breach of Confidentiality Obligations,
(d) Regulatory or statutory fines imposed by a government or Regulatory agency for non-compliance of statutory or regulatory guidelines applicable to the Bank, provided such guidelines were brought to the notice of Service Provider.

For the purpose of clause *31(iii)(b)* **"Gross Negligence" means** any act or failure to act by a party which was in reckless disregard of or gross indifference to the obligation of the party under this Agreement and which causes injury, damage to life, personal safety, real property, harmful consequences to the other party, which such party knew, or would have known if it was acting as a reasonable person, would result from such act or failure to act for which such Party is legally liable. Notwithstanding the forgoing, Gross Negligence shall not include any action taken in good faith. **"Willful Misconduct" means** any act or failure to act with an intentional disregard of any provision of this Agreement, which a party knew or should have known if it was acting as a reasonable person, which would result in injury, damage to life, personal safety, real property, harmful consequences to the other party, but shall not include any error of judgment or mistake made in good faith.

28. CONFIDENTIALITY:

Confidentiality obligation shall be as per non-disclosure agreement (NDA) and Master Service Level Agreement (MSLA) with Bank.

29. DELAY IN SERVICE PROVIDER'S PERFORMANCE:

i. Services shall be made by Service Provider within the timelines prescribed in part II of this document.

ii. If at any time during performance of the Contract, Service Provider should encounter conditions impeding timely delivery and performance of Services, Service Provider shall promptly notify the Bank in writing of the fact of the delay, it's likely duration and cause(s). As soon as practicable after receipt of Service Provider's notice, the Bank shall evaluate the situation and may, at its discretion, extend Service Providers' time for performance, in which case, the extension shall be ratified by the parties by amendment of the Contract.

iii. Any delay in performing the obligation/ defect in performance by Service Provider may result in imposition of penalty, liquidated damages and/or termination of Contract (as laid down elsewhere in this RFP document).

30. SERVICE PROVIDER'S OBLIGATIONS:

i. Service Provider is responsible for and obliged to conduct all contracted activities in accordance with the Contract using state-of-the-art methods and economic principles and exercising all means available to achieve the performance specified in the Contract.

ii. Service Provider is obliged to work closely with the Bank's staff, act within its own authority and abide by directives issued by the Bank from time to time and complete implementation activities.

iii. Service Provider will abide by the job safety measures prevalent in India and will free the Bank from all demands or responsibilities arising from accidents or loss of life, the cause of which is Service Provider's negligence. Service Provider will pay all indemnities arising from such incidents and will not hold the Bank responsible or obligated.

iv. Service Provider is responsible for activities of its personnel or sub-contracted personnel (where permitted) and will hold itself responsible for any misdemeanours.

v. Service Provider shall treat as confidential all data and information about the Bank, obtained in the process of executing its responsibilities, in strict confidence and will not reveal such information to any other party without prior written approval of the Bank as explained under 'Non-Disclosure Agreement' with Bank.

31. INTELLECTUAL PROPERTY RIGHTS AND OWNERSHIP:

i. For any technology / software / product used/supplied by Service Provider for performing Services for the Bank as part of this RFP, Service Provider shall have right to use as well as right to license such technology/ software / product. The Bank shall not be liable for any license or IPR violation on the part of Service Provider.

ii. Without the Bank's prior written approval, Service provider will not, in performing the Services, use or incorporate link to or call or depend in any way upon, any software or other intellectual property that is subject to an Open Source or Copy left license or any other agreement that may give rise to any third-party claims or to limit the Bank's rights under this RFP.

iii. Subject to clause *36 (iv) and 36 (v)* of this RFP, Service Provider shall, at its own expenses without any limitation, indemnify and keep fully and effectively indemnified the Bank against all costs, claims, damages, demands, expenses and liabilities whatsoever nature arising out of or in connection with all claims of infringement of Intellectual Property Right, including patent, trademark, copyright, trade secret or industrial design rights of any third party arising from the Services or use of the technology / software / products or any part thereof in India or abroad.

iv. The Bank will give (a) notice to Service Provider of any such claim without delay/provide reasonable assistance to Service Provider in disposing of the claim; (b) sole authority to defend and settle such claim and; (c) will at no time admit to any liability for or express any intent to settle the claim provided that (i) Service Provider shall not partially settle any such claim without the written consent of the Bank, unless such settlement releases the Bank fully from such claim, (ii) Service Provider shall promptly provide the Bank with copies of all pleadings or similar documents relating to any such claim, (iii) Service Provider shall consult with the Bank with respect to the defence and settlement of any such claim, and (iv) in any litigation to which the Bank is also a party, the Bank shall be entitled to be separately represented at its own expenses by counsel of its own selection.

v. Service Provider shall have no obligations with respect to any infringement claims to the extent that the infringement claim arises or results from: (i) Service Provider's compliance with the Bank's specific technical designs or instructions (except where Service Provider knew or should have known that such compliance was likely to result in an infringement claim and Service Provider did not inform the Bank of the same); or (ii) any unauthorized modification or alteration of the deliverable (if any) by the Bank.

vi. Service provider agrees that the Bank owns the entire right, title and interest to any inventions, designs, discoveries, writings and works of authorship, including all intellectual property rights, copyrights. Any work made under this RFP shall be deemed to be 'work made for hire' under any Indian/U.S. or any other applicable copyright laws.

vii. The Intellectual Property Rights on the software code, copyright and source code for various applications/ interfaces developed under this RFP, and any other component/ framework/ middleware used/ developed as pre-built software assets to deliver the solution, shall belong to the Bank and the Bank shall have complete and unrestricted rights on such property. However, Service Provider shall hold All Intellectual Property rights in any pre-built software *per se*, except for those which have been assigned under this RFP.

viii. All information processed by Service provider during software maintenance belongs to the Bank. Service provider shall not acquire any other right in respect of the information for the license to the rights owned by the Bank. Service provider will implement mutually agreed controls to protect the information. Service provider also agrees that it will protect the information

appropriately.

32. LIQUIDATED DAMAGES:

If Service Provider fails to deliver and perform any or all the Services within the stipulated time, schedule as specified in this RFP/Agreement, the Bank may, without prejudice to its other remedies under the RFP/Agreement, and unless otherwise extension of time is agreed upon without the application of liquidated damages, deduct from the Project Cost, as liquidated damages a sum equivalent to 0.5% of total Project Cost for delay of each week or part thereof maximum up to 5% of total Project Cost. Once the maximum deduction is reached, the Bank may consider termination of the Agreement.

33. CONFLICT OF INTEREST:

i. Bidder shall not have a conflict of interest (the "Conflict of Interest") that affects the bidding Process. Any Bidder found to have a Conflict of Interest shall be disqualified. In the event of disqualification, the Bank shall be entitled to forfeit and appropriate the Bid Security and/or Performance Security (Bank Guarantee), as the case may be, as mutually agreed upon genuine estimated loss and damage likely to be suffered and incurred by the Bank and not by way of penalty for, inter alia, the time, cost and effort of the Bank, including consideration of such Bidder's proposal (the "Damages"), without prejudice to any other right or remedy that may be available to the Bank under the bidding Documents and/ or the Agreement or otherwise.

ii. Without limiting the generality of the above, a Bidder shall be deemed to have a Conflict of Interest affecting the bidding Process, if:

(a) the Bidder, its Member or Associate (or any constituent thereof) and any other Bidder, its Member or any Associate thereof (or any constituent thereof) have common controlling shareholders or other ownership interest; provided that this disqualification shall not apply in cases where the direct or indirect shareholding of a Bidder, its Member or an Associate thereof (or any shareholder thereof having a shareholding of more than 5% (five per cent) of the paid up and subscribed share capital of such Bidder, Member or Associate, as the case may be) in the other Bidder, its Member or Associate, has less than 5% (five per cent) of the subscribed and paid up equity share capital thereof; provided further that this disqualification shall not apply to any ownership by a bank, insurance company, pension fund or a public financial institution referred to in section 2(72) of the Companies Act, 2013. For the purposes of this Clause, indirect shareholding held through one or more intermediate persons shall be computed as follows: (aa) where any intermediary is controlled by a person through management control or otherwise, the entire shareholding held by such controlled intermediary in any other person (the "Subject Person") shall be taken into account for computing the shareholding of such controlling person in the Subject Person; and (bb) subject always to sub-clause (aa) above, where a person does not exercise control over an intermediary, which has shareholding in the

Subject Person, the computation of indirect shareholding of such person in the Subject Person shall be undertaken on a proportionate basis; provided, however, that no such shareholding shall be reckoned under this sub-clause (bb) if the shareholding of such person in the intermediary is less than 26% of the subscribed and paid up equity shareholding of such intermediary; or

(b) a constituent of such Bidder is also a constituent of another Bidder; or

(c) such Bidder, its Member or any Associate thereof receives or has received any direct or indirect subsidy, grant, concessional loan or subordinated debt from any other Bidder, its Member or Associate, or has provided any such subsidy, grant, concessional loan or subordinated debt to any other Bidder, its Member or any Associate thereof; or

(d) such Bidder has the same legal representative for purposes of this Bid as any other Bidder; or

(e) such Bidder, or any Associate thereof, has a relationship with another Bidder, or any Associate thereof, directly or through common third party/ parties, that puts either or both of them in a position to have access to each other's information about, or to influence the Bid of either or each other; or

(f) such Bidder or any of its affiliates thereof has participated as a consultant to the Bank in the preparation of any documents, design or technical specifications of the RFP.

iii. For the purposes of this RFP, Associate means, in relation to the Bidder, a person who controls, is controlled by, or is under the common control with such Bidder (the "Associate"). As used in this definition, the expression "control" means, with respect to a person which is a company or corporation, the ownership, directly or indirectly, of more than 50% (fifty per cent) of the voting shares of such person, and with respect to a person which is not a company or corporation, the power to direct the management and policies of such person by operation of law or by contract.

34. CODE OF INTEGRITY AND DEBARMENT/BANNING:

i. The Bidder and their respective officers, employees, agents and advisers shall observe the highest standard of ethics during the bidding Process. Notwithstanding anything to the contrary contained herein, the Bank shall reject Bid without being liable in any manner whatsoever to the Bidder if it determines that the Bidder has, directly or indirectly or through an agent, engaged in corrupt/fraudulent/coercive/undesirable or restrictive practices in the bidding Process.

ii. Bidders are obliged under code of integrity to Suo-moto proactively declare any conflicts of interest (pre-existing or as and as soon as these arise at any stage) in RFP process or execution of contract. Failure to do so would amount to violation of this code of integrity.

iii. Any Bidder needs to declare any previous transgressions of such a code of integrity with any entity in any country during the last three years or of being debarred by any other procuring entity. Failure to do so would amount to violation of this code of integrity.

iv. For the purposes of this clause, the following terms shall have the meaning hereinafter, respectively assigned to them:

(a) "**Corrupt practice**" means making offers, solicitation or acceptance of bribe, rewards or gifts or any material benefit, in exchange for an unfair advantage in the procurement process or to otherwise influence the procurement process or contract execution.

(b) **"Fraudulent practice"** means any omission or misrepresentation that may mislead or attempt to mislead so that financial or other benefits may be obtained, or an obligation avoided. This includes making false declaration or providing false information for participation in a RFP process or to secure a contract or in execution of the contract;

(c) **"Coercive practice"** means harming or threatening to harm, persons or their property to influence their participation in the procurement process or affect the execution of a contract.

(d) **"Anti-competitive practice"** means any collusion, bid rigging or anti-competitive arrangement, or any other practice coming under the purview of the Competition Act, 2002, between two or more bidders, with or without the knowledge of the Bank, that may impair the transparency, fairness and the progress of the procurement process or to establish bid prices at artificial, non-competitive levels;

(e) **"Obstructive practice"** means materially impede the Bank's or Government agencies investigation into allegations of one or more of the above mentioned prohibited practices either by deliberately destroying, falsifying, altering; or by concealing of evidence material to the investigation; or by making false statements to investigators and/or by threatening, harassing or intimidating any party to prevent it from disclosing its knowledge of matters relevant to the investigation or from pursuing the investigation; or by impeding the Bank's rights of audit or access to information;

v. **Debarment/Banning**

Empanelment/participation of Bidders and their eligibility to participate in the Bank's procurements is subject to compliance with code of integrity and performance in contracts as per terms and conditions of contracts. Following grades of debarment from empanelment/participation in the Bank's procurement process shall be considered against delinquent Vendors/Bidders:

(a) **Holiday Listing (Temporary Debarment - suspension):**

Whenever a Vendor is found lacking in performance, in case of less frequent and less serious misdemeanors, the vendors may be put on a holiday listing (temporary debarment) for a period up to 12 (twelve) months. The vendor on the holiday listing is neither invited to bid nor are his bids considered for evaluation during the period of the holiday. The Vendor is, however, not removed from the list of empaneled vendors, if any. Performance issues which may justify holiday listing of the Vendor are:

- Vendors who have not responded to requests for quotation/tenders consecutively three times without furnishing valid reasons, if mandated in the empanelment contract (if applicable);
- Repeated non-performance or performance below specified standards (including after sales services and maintenance services etc.);

- Vendors undergoing process for removal from empanelment/participation in procurement process or banning/debarment may also be put on a holiday listing during such proceedings.

(b) Debarment from participation including removal from empanelled list

Debarment of a delinquent Vendor (including their related entities) for a period (one to two years) from the Bank's procurements including removal from empanelment, wherever such Vendor is empaneled, due to severe deficiencies in performance or other serious transgressions. Reasons which may justify debarment and/or removal of the Vendor from the list of empaneled vendors are:

- Without prejudice to the rights of the Bank under Clause *39(i)* hereinabove, if a Bidder is found by the Bank to have directly or indirectly or through an agent, engaged or indulged in any corrupt/fraudulent/coercive/undesirable or restrictive practices during the bidding Process, such Bidder shall not be eligible to participate in any EOI/RFP issued by the Bank during a period of 2 (two) years from the date of debarment.
- Vendor fails to abide by the terms and conditions or to maintain the required technical/operational staff/equipment or there is change in its production/service line affecting its performance adversely, or fails to cooperate or qualify in the review for empanelment;
- If Vendor ceases to exist or ceases to operate in the category of requirements for which it is empaneled.
- Bankruptcy or insolvency on the part of the vendor as declared by a court of law; or
- Banning by Ministry/Department or any other Government agency.
- Other than in situations of force majeure, technically qualified Bidder withdraws from the procurement process or after being declared as successful bidder: (i) withdraws from the process; (ii) fails to enter into a Contract; or (iii) fails to provide any other document or security required in terms of the RFP documents;
- If the Central Bureau of Investigation/CVC/C&AG or Vigilance Department of the Bank or any other investigating agency recommends such a course in respect of a case under investigation.
- Employs a Government servant or the Bank's Officer within two years of his retirement, who has had business dealings with him in an official capacity before retirement; or
- Any other ground, based on which the Bank considers, that continuation of Contract is not in public interest.
- If there is strong justification for believing that the partners/directors/proprietor/agents of the firm/company has been guilty of violation of the code of integrity or Integrity Pact (wherever applicable), evasion or habitual default in payment of any tax levied by law; etc.

(c) **Banning from Ministry/Country-wide procurements**

For serious transgression of code of integrity, a delinquent Vendor (including their related entities) may be banned/debarred from participation in a

procurement process of the Bank including procurement process of any procuring entity of Government of India for a period not exceeding three years commencing from the date of debarment.

35. TERMINATION FOR DEFAULT:

i. The Bank may, without prejudice to any other remedy for breach of Agreement, written notice of not less than 30 (thirty) days, terminate the Agreement in whole or in part:
   (a) If Service Provider fails to deliver any or all the obligations within the time period specified in the RFP/Agreement, or any extension thereof granted by the Bank.
   (b) If Service Provider fails to perform any other obligation(s) under the RFP/Agreement.
   (c) Violations of any terms and conditions stipulated in the RFP.
   (d) On happening of any termination event mentioned in the RFP/Agreement.

   Prior to providing a written notice of termination to Service Provider under clause *40 (i) (a) to 40 (i) (c),* the Bank shall provide Service Provider with a written notice of 30 (thirty) days to cure such breach of the Agreement. If the breach continues or remains unrectified after expiry of cure period, the Bank shall have right to initiate action in accordance with above clause.

ii. In the event the Bank terminates the Contract in whole or in part for the breaches attributable to Service Provider, the Bank may procure, upon such terms and in such manner as it deems appropriate, Services similar to those undelivered, and subject to limitation of liability clause of this RFP Service Provider shall be liable to the Bank for any increase in cost for such similar Services. However, Service Provider shall continue performance of the Contract to the extent not terminated.
iii. If the Contract is terminated under any termination clause, Service Provider shall handover all documents/ executable/ Bank's data or any other relevant information to the Bank in timely manner and in proper format as per scope of this RFP and shall also support the orderly transition to another vendor or to the Bank.
iv. During the transition, Service Provider shall also support the Bank on technical queries/support on process implementation.
v. The Bank's right to terminate the Contract will be in addition to the penalties / liquidated damages and other actions as specified in this RFP.
vi. In the event of failure of Service Provider to render the Services or in the event of termination of Agreement or expiry of term or otherwise, without prejudice to any other right, the Bank at its sole discretion may make alternate arrangement for getting the Services contracted with another vendor. In such case, the Bank shall give prior notice to the existing Service Provider. The existing Service Provider shall continue to provide services as per the terms of the Agreement until a 'New Service Provider' completely takes over the work. During the transition phase, the existing Service Provider shall render all reasonable assistance to the new Service Provider within such period prescribed by the Bank, at no extra cost to the Bank, for ensuring smooth switch over and continuity of services, provided where

transition services are required by the Bank or New Service Provider beyond the term of this Agreement, reasons for which are not attributable to Service Provider, payment shall be made to Service Provider for such additional period on the same rates and payment terms as specified in this Agreement. If existing Service Provider is breach of this obligation, they shall be liable for paying a penalty of 10% of the total Project Cost on demand to the Bank, which may be settled from the payment of invoices for the contracted period. Deployment of 50% of required resources by the successful bidder should be done within 15 days from the PO issuance date and remaining resources within 30 days from the PO issuance date. In case of non-deployment of resources, a penalty of 1% of PO amount per week will be levied.

36. FORCE MAJEURE:

i. Notwithstanding the provisions of terms and conditions contained in this RFP, neither party shall be liable for any delay in in performing its obligations herein if and to the extent that such delay is the result of an event of Force Majeure.

ii. For the purposes of this clause, 'Force Majeure' means and includes wars, insurrections, revolution, civil disturbance, riots, terrorist acts, public strikes, hartal, bundh, fires, floods, epidemic, quarantine restrictions, freight embargoes, declared general strikes in relevant industries, Vis Major, acts of Government in their sovereign capacity, impeding reasonable performance of Service Provider and / or Sub-Contractor but does not include any foreseeable events, commercial considerations or those involving fault or negligence on the part of the party claiming Force Majeure.

iii. If a Force Majeure situation arises, Service Provider shall promptly notify the Bank in writing of such condition and the cause thereof. Unless otherwise directed by the Bank in writing, Service Provider shall continue to perform its obligations under the Contract as far as is reasonably practical and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.

iv. If the Force Majeure situation continues beyond 30 (thirty) days, either party shall have the right to terminate the Agreement by giving a notice to the other party. Neither party shall have any penal liability to the other in respect of the termination of the Agreement as a result of an event of Force Majeure. However, Service Provider shall be entitled to receive payments for all services rendered up to the date of the termination of the Agreement.

37. TERMINATION FOR INSOLVENCY:

The Bank may, at any time, terminate the Contract by giving written notice to Service Provider, if Service Provider becomes Bankrupt or insolvent or any application for bankruptcy, insolvency or winding up has been filed against it by any person. In this event, termination will be without compensation to Service Provider, provided that such termination will not prejudice or affect any right of action or remedy, which has accrued or will accrue thereafter to the Bank.

38. TERMINATION FOR CONVENIENCE:

i. The Bank, by written notice of not less than 90 (ninety) days, may terminate the Contract, in whole or in part, for its convenience, provided same shall

not be invoked by the Bank before completion of half of the total Contract period (including the notice period).

ii. In the event of termination of the Agreement for the Bank's convenience, Service Provider shall be entitled to receive payment for the Services rendered (delivered) up to the effective date of termination.

39. DISPUTES / ARBITRATION (APPLICABLE IN CASE OF SUCCESSFUL BIDDER ONLY):

i. All disputes or differences whatsoever arising between the parties out of or in connection with the Contract (including dispute concerning interpretation) or in discharge of any obligation arising out of the Contract (whether during the progress of work or after completion of such work and whether before or after the termination of the Contract, abandonment, or breach of the Contract), shall be settled amicably. If however, the parties are not able to solve them amicably within 30 (thirty) days after dispute occurs as evidenced through the first written communication from any Party notifying the other regarding the disputes, either party (SBI or Service Provider), give written notice to other party clearly setting out there in specific dispute(s) and/or difference(s) and shall be referred to a sole arbitrator mutually agreed upon, and the award made in pursuance thereof shall be binding on the parties. In the absence of consensus about the single arbitrator, the dispute may be referred to an arbitration panel; one to be nominated by each party and the said arbitrators shall nominate a presiding arbitrator, before commencing the arbitration proceedings. The arbitration shall be settled in accordance with the applicable Indian Laws and arbitration proceeding shall be conducted in accordance with Arbitration and Conciliation Act 1996 and any amendment thereto. Any appeal will be subject to the exclusive jurisdiction of courts at Mumbai.

ii. Service Provider shall continue work under the Contract during the arbitration proceedings unless otherwise directed by the Bank or unless the matter is such that the work cannot possibly be continued until the decision of the arbitrator is obtained.

iii. Arbitration proceeding shall be held at Mumbai, India, and the language of the arbitration proceedings and that of all documents and communications between the parties shall be in English.

40. GOVERNING LANGUAGE:

The governing language shall be English.

41. APPLICABLE LAW:

The Contract shall be interpreted in accordance with the laws of the Union of India and shall be subjected to the exclusive jurisdiction of courts at Mumbai.

42. TAXES AND DUTIES:

i. Service Provider shall be liable to pay all corporate taxes and income tax that shall be levied according to the laws and regulations applicable from time to time in India and the price Bid by Service Provider shall include all such taxes in the quoted price.

ii. Only specified taxes/ levies and duties will be payable by the Bank on

actuals upon production of original receipt wherever required. If any specified taxes/ levies and duties are replaced by the new legislation of Government, same shall be borne by the Bank. The Bank shall not be liable for payment of those Central / State Government taxes, levies, duties or any tax/ duties imposed by local bodies/ authorities, which are not specified by the Bidder.

iii. Prices payable to Service Provider 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, any upward revision in Custom duty.

iv. Income / Corporate Taxes in India: The Bidder shall be liable to pay all corporate taxes and income tax that shall be levied according to the laws and regulations applicable from time to time in India and the price Bid by the Bidder shall include all such taxes in the contract price.

v. All expenses, stamp duty and other charges/ expenses in connection with the execution of the Agreement as a result of this RFP process shall be borne by Service Provider. The Agreement/ Contract would be stamped as per Maharashtra Stamp Act, 1958 and any amendment thereto.

43. TAX DEDUCTION AT SOURCE:

i. Wherever the laws and regulations require deduction of such taxes at the source of payment, the Bank shall effect such deductions from the payment due to Service Provider. The remittance of amounts so deducted and issuance of certificate for such deductions shall be made by the Bank as per the laws and regulations for the time being in force. Nothing in the Contract shall relieve Service Provider from his responsibility to pay any tax that may be levied in India on income and profits made by Service Provider in respect of this Contract.

ii. Service Provider's staff, personnel and labour will be liable to pay personal income taxes in India in respect of such of their salaries and wages as are chargeable under the laws and regulations for the time being in force, and Service Provider shall perform such duties in regard to such deductions thereof as may be imposed on him by such laws and regulations.

44. NOTICES:

Any notice given by one party to the other pursuant to this contract shall be sent to the other party in writing or by Fax and confirmed in writing to other Party's address. For all notices, the following shall be the current address:

The Chief Information Security Officer (ISO),
Information Security Department,
Ground Floor, A Wing
State Bank Global IT Centre
Sector 11, CBD Belapur
Navi Mumbai – 400 614

Email : ciso@sbi.co.in

The notice shall be effective when delivered or on the notice's effective date whichever is later.

Part-II

Appendix –A

BID FORM

[On Company's letter head]
(To be included in Bid Document)

Date:_____

To:
Dy. General Manager (ISO)
State Bank of India
Information Security Department,
State Bank Global IT Centre,
Ground Floor, A Wing, Sector 11,
CBD Belapur, Navi Mumbai-400614

Dear Sir,

REQUEST FOR PROPOSAL (RFP) FOR EMPANELMENT OF INFORMATION SECURITY SERVICE PROVIDERS (ISSP)

We have examined the above RFP, the receipt of which is hereby duly acknowledged and subsequent pre-bid clarifications/ modifications / revisions, if any, furnished by the Bank and we offer to provide Services detailed in this RFP.

We shall abide by the terms and conditions spelt out in the RFP.

i. While submitting this Bid, we certify that:

- The undersigned is authorized to sign on behalf of the Bidder and the necessary support document delegating this authority is enclosed to this letter.
- We declare that we are not in contravention of conflict of interest obligation mentioned in this RFP.
- We have not induced or attempted to induce any other Bidder to submit or not to submit a Bid for restricting competition.

ii. We understand that this RFP is not an offer by State Bank of India, but an invitation to receive responses from the Bidders. No contractual obligation whatsoever shall arise from the RFP process unless and until a formal contract is signed and executed by duly authorized official(s) of State Bank of India with the selected Bidders.

iii. We undertake that, in competing for (and, if the award is made to us, in executing) the above contract, we will strictly observe the laws against fraud and corruption in force in India namely "Prevention of Corruption Act 1988".

iv. We undertake that we will not offer, directly or through intermediaries, any bribe, gift, consideration, reward, favor, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the Bank, connected directly or indirectly with the bidding process, or to any person, organization or third

party related to the contract in exchange for any advantage in the bidding, evaluation, contracting and implementation of the contract.

v. We undertake that we will not resort to canvassing with any official of the Bank, connected directly or indirectly with the bidding process to derive any undue advantage. We also understand that any violation in this regard, will result in disqualification of bidder from further bidding process.

vi. It is further certified that the contents of our Bid are factually correct. We have not sought any deviation to the terms and conditions of the RFP. We also accept that in the event of any information / data / proving to be incorrect, the Bank will have right to disqualify us from the RFP without prejudice to any other rights available to the Bank.

vii. We certify that while submitting our Bid document, we have not made any changes in the contents of the RFP document, read with its amendments/clarifications provided by the Bank.

viii. We agree to abide by all the RFP terms and conditions, contents of Master Service Level Agreement with Bank and the rates quoted therein for the orders awarded by the Bank up to the period prescribed in the RFP, which shall remain binding upon us.

ix. On acceptance of our technical bid, and in case of declaration as successful Bidder on completion of Technical evaluation, we undertake to complete the formalities as specified in this RFP.

x. Till execution of a formal contract, the RFP, along with the Bank's notification of award by way of issuance of purchase order and our acceptance thereof, would be binding contractual obligation on the Bank and us.

xi. We understand that you are not bound to accept the lowest or any Bid you may receive, and you may reject all or any Bid without assigning any reason or giving any explanation whatsoever.

xii. We hereby certify that our name does not appear in any "Caution" list of RBI / IBA or any other regulatory body for outsourcing activity.

xiii. We hereby certify that on the date of submission of Bid for this RFP, we are not under any debarment/blacklist period for breach of contract/fraud/corrupt practices by any Scheduled Commercial Bank/ Public Sector Undertaking/ State or Central Government or their agencies/departments.

xiv. We hereby certify that on the date of submission of Bid, we do not have any Master Service Level Agreement pending to be signed with the Bank for more than 6 months from the date of issue of purchase order.

xv. We hereby certify that we have read the clauses contained in O.M. No. 6/18/2019-PPD, dated 23.07.2020 order (Public Procurement No. 1), order (Public Procurement No. 2) dated 23.07.2020 and order (Public Procurement No.

3) dated 24.07.2020 regarding restrictions on procurement from a bidder of a country which shares a land border with India. We further certify that we are not from such a country or if from a country, have been registered with competent authority. We certify that we fulfill all the requirements in this regard and are eligible to participate in this RFP.

xvi. If our Bid is accepted, we undertake to enter into and execute at our cost, when called upon by the Bank to do so, a contract in the prescribed form and we shall be solely responsible for the due performance of the contract.

xvii. We furnish hereunder the details of the authorized person who would be contacted for any clarifications on bid submitted.

Name of the authorized person:

Phone/Mobile No.

E-mail ID:

xviii. We, further, hereby undertake and agree to abide by all the terms and conditions stipulated by the Bank in the RFP document.

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.

Appendix-B

SCOPE OF WORK

1. The scope mentioned below is illustrative but not exhaustive. Bidders are expected to update and include additional relevant items in these activities to conform to global best practices, currently available knowledge base, emerging threats to IT, Information and Cyber Security, latest security solutions like DLP, NAC, anti APT solution, anti-malware etc.

Common Deliverables

- Clarifications
- Discussions
- References / Rationale for recommendations

Reports would be in –

- soft copies
- Signed hard copies – Two numbers
- copies of screen shots,
- outputs,
- Review evidence
- soft outputs which are importable into a database, spreadsheet, or GRC platform e.g. XML files, CSV files etc.
- Tracking sheet
- PowerPoint presentation for Top management
- Vulnerabilities identified
- Ease of exploitation of vulnerability
- CVE, CWE, CPE, CVSS scores, as applicable
- Vulnerability ratings
- Threat Profile
- Test Plan
- Compliance profile covering compliance with Banks policies, legal and regulatory requirements and industry best practices, whichever are the best (inclusive of RBI guidelines on Information/Cyber Security dated 29.04.2011 and 02.06.2016 and any subsequent domestic and foreign regulatory guidelines issued etc.)
- Compliance requirements where applicable
- Screenshots and code listing or line numbers where feasible in code reviews
- Solutions with details and additional resources.

II. **Service Types:**

Services are categorised into two areas viz.

II.A. Standardised and
II.B. Specialised.

Detailed descriptions of the services are given in the subsequent sections.

Bidders are also required to indicate the service priority list – Annexure C10 - based on their skills, competencies, experience, ability and willingness to offer specific services in order of priority.

II.A. Standardized Service

The ISSP mandated to conduct security review is expected to conduct comprehensive techno-operational-functional-process-security review of systems under the scope of work and the report submitted by them must be comprehensive, factual and evidence based including but not limited to –

- details of each system covered in the scope of such review.
- screenshots, logs, diagrams, data and attack flow diagram, artefacts, forensic related information
- network, security and IT assets, protocols, ports, topology etc. which could potentially be compromised.
- attack vector or group of attack vectors, order / seriatim of attack vectors which could compromise the systems.
- CVE, CWE, CPE, CVSS etc.
- specific patches, versions, signatures, firewall / router / switch configurations & rules, configuration, work around, quick fix, compensatory control required to protect the information process asset(s) from exploitation of reported vulnerability / attack.
- probability of attack, tools/scripts required to exploit, ease (complexity) of attack, ease of exploit, probability of exploitation of vulnerability, cascading effect of vulnerability on the systems.
- specific controls / control objective in ISO, PCI-DSS standards, RFC, OWASP, COBIT, domestic and foreign regulatory instructions / circulars / guidelines / recommendations / prescriptions (as applicable) which is (may get) violated due to techno-functional-process vulnerability.
- violates / impacts which information security pillar – confidentiality, integrity, availability, authentication, authorisation, non-repudiation etc.
- recommendations specific to the Bank's environment under security review
- avoid generic and speculative recommendations.
- share and discuss draft observations with ISD/Application Owner as and when mandated by them.
- make presentations to stakeholders on observations submitted as required by the Bank from time to time.
- Framework for each of the below assessment first be demonstrated to the Bank for approval and the same should be followed. Changes in the assessment framework should be proposed by the ISSP from time to time (at least annually), keeping them aligned with the global standards. No extra commercials shall be paid by the Bank for adopting revised assessment standards.
- Bank may on its own mandate to adopt new / revised assessment standards from time to time. The same shall be binding on the ISSPs, without any extra commercials.
- ISSPs should make half yearly presentation to the Bank's top management on information security landscape of the Bank as assessed over a period of time vis-à-vis global banks, domestic and foreign regulatory mandates, as

also should recommend areas of improvement. Such presentations should be made by Partners or similar level top executives of ISSP.

II.A.1. Vulnerability Assessment

SBI expects an authenticated type but non-destructive internal and external vulnerability assessment to be carried out. Bidder should be able to cover a broad range of systems, but not limited to Operating system (Windows, Linux, AIX, HP UX etc), Databases (MSSQL, Oracle, Front DB, MongoDB etc), Web servers (Apache, Tomcat, IIS etc), Network devices (Cisco, Juniper etc), Security devices (Cisco, Checkpoint, Juniper, SonicWALL etc), Virtualization, Cloud environment, various applications like AD, AV, DLP, NAC, PIMS, IAM, ACC, FIM, SSO, SOC and business applications like Core Banking, Internet Banking, Mobile Banking, ATM, Treasury etc. The security review should cover comprehensive assessment of technological, functional, processes associated with the system and IT/digital and information and cyber security ecosystem associated with systems under the scope of such review. Vulnerability Assessment should include uncover vulnerabilities which could potentially be exploited without logging into the systems and post login (administrative credential based).

Bidders are expected to conduct the security review against the standard security configuration documents that bank has created, as also the latest global standards and industry best practices. In case, any new information system / asset is identified during project execution, the bidder is expected to develop the checklist and conduct the assessment thereof.

Broad scope of work for Vulnerability Assessment

1 General aspects for all systems
- Access control and authentication
- Network settings
- General system and security configuration
- Logging and auditing
- Password and account policies
- Patches and updates etc.

2 Specific requirements for Server/OS Configuration review
- File system security and Integrity
- Account Policies
- Access Control
- Network Settings
- System Authentication
- Logging and Auditing
- Patches and Updates
- Unnecessary services
- Remote login settings etc.

3 Configuration review of Networking & Security Devices
- Access Control

- System Authentication
- Auditing and Logging
- Insecure Dynamic Routing Configuration
- Insecure Service Configuration
- Insecure TCP/IP Parameters
- System Insecurities
- Unnecessary services
- Remote login settings
- Latest software version and patches
- Traffic analysis

4 Database Configuration security review
- Database Account Authentication
- Password Policy
- Database Account Privileges
- Database Auditing
- Database Logging and Tracing
- Database Network Access Mechanism
- Database Patching
- Database Files and Directories Permission
- Access control and authentication
- Unnecessary services
- Remote login settings
- Patches and updates

5 Security configuration of desktops and laptops that are used by the business users can be performed on sampling basis as per Bank's requirements.

6 Above activities are indicative in nature; the actual scope of activities should be defined by ISSP professionals after considering best practices, actual IT implementation of project, after submission to Bank for it's approval.

Deliverables

Individual report should be provided for each of servers, network & security systems / devices, and other security reviewed systems/processes. Recommend revised and new security configurations, basis the global best practices.

II.A.2. Penetration testing

The objective of the assessment is to determine the effectiveness of the security of Bank's information processing infrastructure and its ability to withstand an intrusion attempt from external and from within the Bank. This may be achieved by conducting both reconnaissance and a comprehensive penetration test. The report should provide good insight as to what an attacker can discover about the network, security systems, information processing systems and how this information can be used to further leverage attacks. Penetration Testing should uncover pre and post login vulnerabilities which could potentially be exploited by external and internal adversary. The security assessment should use the industry standard penetration test methodologies (like OSSTM) and scanning techniques and will focus on

applications. The application tests should cover but not limited to OWASP Top 10 attacks.

Scope of work for Penetration Testing

1. Tests for default passwords
2. Tests for DoS vulnerabilities
3. Test for DDoS vulnerabilities
4. Test for directory Traversal
5. Test for insecure services such as SNMP
6. Check for vulnerabilities based on version of device/server.
7. Test for SQL, XSS and other web application related vulnerabilities
8. Check for weak encryption.
9. Check for weak hashing.
10. Check for SMTP related vulnerabilities such as open mail relay.
11. Check for strong authentication scheme.
12. Test for sample and default applications/pages
13. Check for DNS related vulnerabilities such as DNS cache poisoning and snooping.
14. Test for information disclosure such as internal IP disclosure
15. Look for potential backdoors.
16. Check for older vulnerable version.
17. Remote code execution
18. Weak SSL Certificate and Ciphers
19. Missing patches and versions
20. Test for Insecure Direct Object Reference (IDOR) vulnerabilities.
21. Test for session replay attacks.
22. This is a minimum indicative list, bidders are encouraged to check for more settings in line with best practices including PCI, OSSTM etc

Deliverables

Detailed technical Penetration Test report should be provided containing:

- Executive Summary – Summarize the scope, critical findings, the positive security aspects identified in a manner suitable for the management.
- Categorization of vulnerabilities based on risk level – The report should classify the vulnerabilities as High/Medium/Low based on the Impact and Ease of Exploitation.
- Detail of all test cases attempted during the process of assessment.
- Details of the security vulnerabilities discovered during the review – The detailed findings should be brought out in the report which will cover the details in all aspects.
- Solutions for the discovered vulnerabilities – The report should contain emergency quick fix solutions and long-term solutions based on industry standards.

II.A.3. Technical creation of standard hardening document

Creation of standard hardening document –

The vendor is expected to create a baseline Secured Configuration document (SCD) with parameters, values etc. and descriptions of risks to enable an OS, web

/ application server, network, security, platform, application, database, middleware etc. to be securely configured for use in the Bank.

Scope of work

This document will need to be based on the global standards, documentation available, OEM/Vendor advisories and documents and incidents / vulnerabilities related information available in the public domain / vendor's own knowledge base and experience, integration of asset type, make and model with Bank's SOC, Bank's various policies, domestic and foreign regulatory mandates, ISO, PCI-DSS standards, COBIT framework etc. This will also be required to be updated annually and more frequently in case of need /discovery of new vulnerabilities etc.

Bank may require creating customised SCDs e.g. for desktops (say for CBS, Swayam Passbook printers, ATMs), Windows Servers for a specific / group of applications (say CBS etc) which may require to deviate from standard best practices; in such cases, ISSP should recommend compensatory controls to safeguard such platforms from potential exploitation by external (and internal) adversaries.

Deliverables

A document with all the settings with executable scripts for automatic verification of configuration, requirements and recommendations. Assist the SOC to configure Bank's Vulnerability Management tool to probe the systems pre and post login to fetch these configurations and highlight the gaps / exceptions / misconfigurations.

II.A.4. General Process Review

Assess whether the data processing that takes place in information processing systems occur in a controlled environment, supporting confidentiality, integrity, availability, non-repudiation and security standards as also are in accordance with the Bank's various policies, domestic and foreign regulatory mandates, ISO, PCI-DSS standards, COBIT framework etc.

Scope of work for general process review

The activity includes detailed assessment of the following:

- Assess the controls implemented in the system for Input, Processing, Output, Functionality etc.
- Logical Access Controls - Review all types of Application-Level Access Controls including proper controls for access logs and audit trails for ensuring Sufficiency & Security of Creation, Maintenance and Backup of the same. Only authorized users should be able to edit, input or update data in the applications or carry out activities as per their role and/or functional requirements.
- Assess sufficiency & accuracy of event logging, adequacy of Audit trails, SQL command prompt usage, database level logging, comprehensiveness and correctness of logs collated by SOC from systems under review etc.
- Assess interface controls - Application interfaces with other applications and security in their data communication.

- Assess authorization controls such as Maker Checker, Exceptions, Overriding exception & Error condition.
- Assess Data integrity & File Continuity Controls
- Assess controls for user maintenance, password policies are being followed are as per bank's IT and IS policies with special attention to the use of hardcoded User Id & Password
- Assess controls for segregation of duties and accesses of production staff and development staff with access control over development, test and production regions.
- Review of all types of Parameter maintenance and controls implemented.
- Assess controls for change management procedures including testing & documentation of change.
- Identify gaps in the application security parameter setup in line with the bank's security policies and leading best practices.
- Assess management controls including systems configuration/ parameterization & systems development.
- Assess controls over operations including communication network, data preparation and entry, production, file library, documentation and program library, Help Desk and technical support, capacity planning and performance, Monitoring of outsourced operations.
- Review IT, SOC, Cyber Security incident management mechanism by asset owners
- Review of customizations done to the Software & the SDLC Policy followed for such customization.
- Verify adherence to Legal, Regulatory & Statutory Requirements
- Provide suggestions for segregations of Roles/Responsibilities with respect to Application software to improve internal controls.
- Review of documentation for formal naming standards, design process of job roles, activity, groups, profiles, assignment, approval & periodic review of user profiles, assignment & use of Super user access.
- Check the sufficiency and coverage of UAT test cases, review of defects & tracking mechanism deployed by vendor & resolution including re-testing & acceptance.
- Backup/Fall-back/Restoration /Recovery & Restart procedures

The above should be done in consonance with standards like ISO 27001, ISO 22301, PCI-DSS, COBIT, Bank's IT, IS and Cyber Security Policies, legal, domestic & foreign regulatory & statutory requirements and global best practices.

Deliverables
Detailed findings and recommendation to address each finding, vulnerability, observation in the report.

II.A.5. Review of General IT Controls
Assess whether the data processing that takes place in information processing systems, occurs in a securely controlled environment, supporting data integrity, confidentiality and aspects of techno-operational-functional-process-security.

Scope of work for General IT Controls Review –

1. **Change Management**- To provide reasonable assurance that only appropriately authorized, tested, and approved changes are made to in-scope systems. The following attributes need to be reviewed with appropriate evidences:
   a. All changes are authorized, tested, approved and monitored.
   b. Responsibilities are appropriately segregated.
   c. Rollback plan
   d. Procedures for Emergency changes

2. **Logical Access**- To determine that only authorized persons have access to data and applications (including programs, tables, and related resources) and that they can perform only specifically authorized functions. The following attributes needs to be tested with appropriate evidences:
   a. General Security settings with respect to Application, Operating System, and Database
   b. Privilege User Management
   c. Procedures for New User setup, Terminated Users, Transfers
   d. User Access Reviews
   e. Segregation of Duties

3. **Backup Management**- To determine that the data supporting business information is properly and securely backed-up so that it can be accurately and completely recovered if there is a system outage or data integrity issue. The following attributes needs to be tested with appropriate evidence:
   a. Backup and Recovery
   b. Job Scheduling
   c. Backup encryption

4. **Entity Level Controls**: To determine the adequacy of internal controls that help ensure that management directives pertaining to the entire entity are carried out. The following attributes needs to be tested with appropriate evidences:
   a. Quality Assurance Management process review
   b. Management review and governance over systems performance
   c. Presence of adequate policy and procedures documents and its adherence
   d. Review of previous audit/test reports and the actions taken on the recommendations

5. **Others: Review the following**: -
   a. Audit logging and review mechanism
   b. Patch Management procedures
   c. Antivirus management

Deliverables

Provide report of findings and recommendations. The report should be prepared keeping the following points in view: -

- Identification of gaps/deviancies/deficiencies/vulnerabilities/risks and detailed observations and its potential impact on the business

- Industry best practices
- Specific recommendations for improvement
- Adequate verifiable audit evidences

II.A.6. Vendor Risk Assessment

Scope of Work
IT and operational controls
Outsourcing of critical functions related to IT and Business should be assessed and should include –

- To assess Information Security Risk in Outsourced Vendor Operations
- To assess veracity of IT Security Controls mandated by the Bank
- To conduct risk assessment of all outsourced vendors carrying out key operational processes for Bank vis-à-vis ISO 27001:2013 standard
- To assess whether outsourced vendors meet/incorporate adequate level of security controls commensurate with the business information they receive/ store/process from or on behalf of Bank.
- To assess whether the outsourced vendors comply with the IS Policy of the organization wherever applicable.
- To assess adequacy of privacy and data protection controls at vendor premises

Deliverables
Reports on the above areas with recommendations

II.B. Specialized Services

II.B.1. IS Program Management

Scope of Work
- Supporting monitoring of all information security related activities
- Maintaining overall data
- Providing snapshots, dashboards, tracking
- Continuously scanning external environment

Deliverables
- Dashboards,
- Portal
- MIS
- Tracking
- Presentations
- Advisories

II.B.2. Log Monitoring

Scope of Work

- Monitoring logs
- Providing alerts,
- Storage,
- Correlation through SIEM solutions and add-on tools
- Assistance in mitigation
- Tracking & Closure of incidents

Deliverables

- Alerts
- Mitigation recommendations
- Vendor will be expected to provide help desk – voice/email/portal-based support for some of the services.
- This should include escalation matrix. The availability of this service should be commensurate with the type of service like 24*7 log monitoring.
- Vendor should provide requisite reports including dashboard etc.
- Regulatory / Compliance Requirements
- Vendor should provide requisite reports for the above.
- Security Requirements
- All the services provided by the vendor should conform to the security best practices.

II.B.3. Information Security Awareness

Scope of Work

- General Information Security Awareness
- Specialised Information Security Training to different signings like branch users, users at administrative offices, Senior Management, Top Management, Board of Directors, Bank's business partners and customers of all categories

Deliverables

- Content creation – presentations, audio, video, eLearning content, quizzes
- Conducting training/awareness sessions

II.B.4. Application Security

Scope of Work for Application Security Assessment

Technical Assessment

1 The assessment should cover both business and technical risks.
2 The assessment report should contain a detailed threat list of the application. The threat list should contain the possible risks to the application both from a business and technical aspect.
3 The tester should attempt to identify and exploit vulnerabilities that include the OWASP Top 10, including (not limited to top 10 only. The tester may be required to identify other OWASP vulnerabilities also):
   - Input validation

- Cross site scripting
- SQL injection
- Cookie modification
- Code execution
- Buffer overflow
- URL manipulation
- Authentication bypass
- File upload vulnerabilities
- IDOR vulnerability /server-side validation
- Secure implementation of features such as forgot password, password policies enforcement, CAPTCHA etc
- Session hijacking/session replay
- CSRF
- Privilege escalation

4 The report should show risk to the business based on any exploits that was found.

5 The assessment report should contain a test plan that shows what tests were conducted and its status.

Process Assessment

1 Authorization and Segregation of Duties Controls
- Understand how system entitlements are used to enforce segregation of duties or authorized transactions.
- Perform sample testing of user application entitlements to confirm appropriate segregations of duties are enforced by the system (in a test environment).
- Perform sample testing of user application entitlement to ensure access to enter, approve, and/or modify transactions, data, or system configurations is restricted to authorized personnel (in a test environment).
- Populate issue and findings log with the gaps / deviations / issues noted (if any)

2 Assessment of Role based Security for Applications under scope.
- Review of user creation/modification/deletion/maintenance procedures for the in-scope applications
- Review of privileged access rights granted to application, system administrators, service providers and vendors.
- Assess the process for review of user logs for administrator and system users.
- Review ongoing monitoring of effectiveness of implemented procedures and controls.
- Perform sample testing of application entitlement to ensure access to enter, approve, and/or modify transactions, data, or system configurations is restricted to authorized personnel.
- Review of account and password policy including controls such as
- Users are assigned unique accounts.
- Adequate passwords are maintained e.g., alphanumeric, minimum number of characters. etc
- Password policy as per Bank’s IS Policy is followed and

- Review of implementation of password policy at system and application levels
- Account lockout policy for disabling user accounts after limited number of unsuccessful login attempts
- Segregation of duties controls /maker-checker controls through appropriate design and implementation of user roles / profiles.
- Understand how system entitlements are used to enforce segregation of duties or authorized transactions.
- Perform sample testing of application's entitlements to confirm appropriate segregations of duties are enforced by the system (in a test environment).
- Understand how unsuccessful access attempts to applications in scope are logged and monitored.
- Review the implementation and effectiveness of user access management in applications in the event of leaves.
- Review the segregation of development, production and test environments of applications.
- Understand the manpower deployment for application maintenance.
- Based on the control design weaknesses identified above, identify the areas for conducting forensic study.

3 Others

- Review the audit trail features of the applications in scope, understand how the audit trail reports are reviewed by SBI to detect errors and understand how the reported errors are corrected in a timely manner.
- Review the maintenance and storage of audit trails and logs to assess whether the same can be used for forensic study if required by SBI
- Understand the legal and statutory requirements related to using the applications in scope
- Review other related procedures namely backup, change management, Escrow arrangement for source code and risk management processes for the applications in scope.

Deliverables

- Identified threats for each application.
- Report of findings and recommendations for each application.
- All the reports would be prepared module/functionality-wise keeping the following points in view.:
    - The assurance that application functions as intended by SBI's information security policy.
    - Identification of gaps/deviancies/deficiencies/vulnerabilities/risks and detailed observations and its potential impact on the business
    - Industry best practices
    - Specific recommendations for improvement
    - Adequate verifiable audit evidence
- Security and control review report of the applications in scope
- All observations will be thoroughly discussed with team/application owners before finalization of report and the users' views/explanations to be noted for deviations/recommendations. However, this should not influence the independent views/observations of the auditors.

- All the documents and audit evidences, documentary or otherwise with screenshots/gist of discussion with stakeholders

II.B.5. Code Review

The code review activity should help the bank in uncovering any vulnerability that an adversary may potentially exploit

Scope of Work for Code Review

- Conduct in-depth understanding of the application architecture
- Prepare a threat profile listing all threats that are applicable to the in-scope application
- Study the code layout in terms of pages, classes, modules, interfaces and custom protocols
- Conduct manual and automated code review (Black Box, Grey Box or White Box, as the case may be) as per criticality of the code using the latest tool(s).
- Use combination of tools like custom scripts, static code analysers, process, file and registry usage monitors, dis-assemblers, de-compliers etc.
- Verify the findings reported by the tools and prioritize them based on their criticality and impact
- The clauses for verification of Code review submitted by other CERT-IN empanelled ISSP may also be required and should be reviewed independently by Bank's engaged ISSP for submission of their opinion to Bank for its acceptability or limitation etc.

Deliverables

The code review report should contain the following at minimum:

- Vulnerabilities identified
- Vulnerability ratings
- Threat Profile
- Test Plan
- Compliance requirements where applicable
- Screenshots and code listing or line numbers where feasible
- Solutions with details and additional resources.

II.B.6. BCP / DRP

SBI wants to implement a comprehensive continuity management program which will comprise of detailed business impact analysis and development to business and IT strategies. This will be followed by the development and SBI wide response plans.

Activities under BCM

1. Systems Study
   - Read the existing BCP policy of SBI and review it against leading practices to identify gaps.
   - Benchmark it with the requirements of standards such as BS25999
   - Discuss the recommendations with the SBI and assist in documenting the new policy and associated processes / documents based on the recommendations accepted by SBI

2. Assist in documenting a high-level roadmap and timeframe for the BCP engagement
   - Understand the business operations of SBI including the processes, underlying IT infrastructure and locations
   - Identify key activities to be carried out as part of the BCP engagement
   - Mutually decide the deliverables and resource plan of the project and collect relevant documents, information and data
   - Conduct Kick-off workshop with business process owners to provide overview of the project, overview of Business Impact Analysis (BIA), Recovery objectives etc.
3. Business Impact Analysis
   - For the identified locations and business units, conduct detailed discussions with the relevant stakeholders to populate the BIA document. The BIA should necessarily:
   - Identify critical business functions/processes, their resource requirements and interdependencies
   - Estimate the financial and operational impacts of disruptions
   - Determine the recovery time objective (RTO) and recovery point objective (RPO) for mission critical functions
   - The business impacts should be assessed keeping in mind the following:
     - The impact on staff or public wellbeing;
     - The impact of damage to, or loss of, premises, technology or information;
     - The impact of breaches of statutory duties or regulatory requirements;
     - Damage to reputation;
     - Damage to financial viability;
     - Deterioration of product or service quality;
     - Environmental damage.
   - Discuss with management the approach for assessing the impact of disruption and present the findings and conclusions.
   - Review the results of business impact assessment, recovery time objectives for operations and recovery point objectives for data and systems, and validate for consistency and incorporation of accepted inputs
   - Estimate the resource requirements for each critical activity after resumption taking the following into account:
     - Staff resources, including numbers, skills and knowledge (people);
     - The works site and facilities required (premises);
     - Supporting technology, plant and equipment (technology);
     - Provision of information (whether electronic or paper-based) about previous work or current work-in-progress, all of which is sufficiently up-to-date and accurate to allow the activity to continue effectively at the agreed level (information); and
     - External services and suppliers (supplies).
   - Undertake a Risk assessment exercise in consultation with relevant stakeholders:
     - Determine the criteria for risk acceptance.
     - Identify acceptable level of risks
     - Analyse the risks
     - Evaluate threats and vulnerabilities

    - Assess impacts that might result from exploitation of vulnerabilities by threats.
  - Identify the most probable threats to the organization and or location within the organization and analyse the related vulnerabilities of the organization to those threats
  - Evaluate the existing physical and environmental security and controls and assess their adequacy relative to the potential threats of the organization
  - Evaluate the risk mitigation strategies
  - Provide a findings / recommendations report to management
4. BCM Strategy
  - Determine and guide SBI in the selection of alternative business recovery operating strategies for recovery of business operations within the recovery time objectives, while maintaining the organization's critical functions.
  - Identify and document recovery strategies for each line of mission critical business functions based on RTO/ RPO after discussion with the stakeholders
  - Deliberate with the management of SBI and assist in determining the relative costs for implementing strategies and provide cost benefit analysis
5. IT Strategy
  - Provide high level strategy guidance for IT systems to fulfil the recovery objectives
  - Provide guidance for improving the organization's DR strategy.
6. BCM Planning and plan development
  - Create and document detailed plans including business resumption, site restoration, crisis management, technology recovery and critical staff management, communication plan etc.
  - Document roles and responsibilities of people and teams having authority (both in terms of decision-making and authority to spend) during and following an incident.
  - Define the purpose and scope of each specific plan and present it to top management for review.
  - Conduct meetings and awareness sessions for key stakeholders who will put the plan into effect.
  - Establish and document clear guidelines and a set of criteria regarding which individual(s) have the authority to invoke the plan(s) and under what circumstances.
7. Implementation and Training
  - Create the teams and allocate responsibilities in line with BCP
  - Conduct training and awareness sessions for end users
  - Assist SBI in implementing procedural and technical measures as per plan
8. BCM Testing and Maintenance
  - Create overall testing and maintenance plan
  - Identify test participants, test dates and test outcomes
  - Develop process for BCM improvement based on test results
9. Certification Support

Deliverables

- Project Plan
- Risk Assessment document

- BIA document
- BCM Strategy documents
- Plan and procedure documents
- Testing and Maintenance plan
- Training program and content document

II.B.7. Security solution consulting

Scope of Work

The Service Provider shall review the requirement for a type of IT security solution. The review shall document the capabilities that would be most appropriate to meet organization needs. The service provider should assemble a list of the type of solutions designed for these needs/or prepare a customised solution requirement. The service provider shall deliver a Solution Requirements Report and Possible Solutions List. For each solution identified as requiring further evaluation, the service provider shall do a POC/comparative evaluation for the solutions either directly or in coordination with the provider of the solution and submit a report with comparison to client giving all solutions. The decision about selection and procurement of the final solution will rest with the Bank. The report shall also address data collection capabilities, utility (e.g., ease of use, error messages, documentation quality), security controls, reporting capabilities, solution support, DFRA, integration with SOC, and compatibility with the organization's other IT security solutions (like PIMS, AD, AV, SSO, ITAM, DLP, SOC etc.) and procedures.

The service provider shall prepare and deliver a report documenting advantages and disadvantages of each solution. The service provider shall prepare a recommendations report on whether solution will meet the organization requirement. Recommendations shall be based on cost, response time, ease of use, ease of implementation and operation, customer support, and quality of documentation.

Deliverables

Various reports capturing the analysis of solutions, evaluation reports, executive summary, management presentations.

II.B.8. Product evaluation

The objective of the activity is to help bank identify and analyse various security products based on requirement and suitability for the bank.

Scope of Work for product evaluation

The Service Provider shall review the requirement for a type of IT security product. The review shall document the capabilities that would be most appropriate to meet organization needs. The service provider should assemble a list of the type of products designed for these needs. The service provider shall deliver a Product Requirements Report and Possible Products List. For each product identified as requiring further evaluation, the service provider shall do a POC for the products either directly or in coordination with the supplier of the project and submit a report with comparison to Bank's requirement of all products. The decision about selection and procurement of the final product will rest with Bank. The report shall also address data collection capabilities, utility (e.g., ease of use, error messages,

documentation quality), security controls, reporting capabilities, product support, and compatibility with the organization's other IT security products and procedures. The service provider shall prepare and deliver a report documenting advantages and disadvantages of each product. The service provider shall prepare a recommendations report on whether product will meet the organization requirement. Recommendations shall be based on cost, response time, ease of use, ease of implementation and operation, customer support, and quality of documentation.

Deliverables

Various reports capturing the analysis of projects, evaluation reports, executive summary, management presentations.

II.B.9. Data Governance

- Ensuring formulation of a scalable and robust Data Classification Framework
- Ensuring templates created are reusable and simplistic
- Ensuring identification of structured and unstructured data
- Ensuring implementation of a lightweight data labelling product for effectively managing unstructured data
- Ensuring identification of granular rule sets for DLP solution implementation

Scope of work

1. Review of existing Data Asset Classification Policy and Methodology
2. Perform data risk assessment to assess security loopholes from where data can get leaked
3. Develop a robust data governance framework which encapsulates:
   - Data Identification
   - Data Classification (PII, SPDI etc.)
   - Records Management as per various domestic and foreign acts, laws and treaties
   - Security control matrix for data at rest (OS, RDBMS etc), in process (RAM, Cache, virtual memory) and in transit (network level encryption, payload encryption, hashing)
   - Secured Data disposal processes
4. Develop Data Classification Guideline and Procedure document (encompassing complete data lifecycle including registration, maintenance, de-classifying and deregistration/ discarding process)
5. To develop training presentations and relevant materials for different audiences such as, business users, technical teams, managers etc.
6. Prepare the Data Classification Project Plan clearly identifying the milestones timelines, approach and resources required.
7. Conduct Data Flow Analyses for the business units across the enterprise
8. Identify key documents & data that need to be classified
9. Identify the supporting applications and corresponding databases for classification and DLP protection.
10. Identify the owner, custodian & authorized users (white listed users)
11. Populating data in Data Classification Repository
12. To create a granular matrix that defines DLP authorization for individual user (Employee) and DLP channels (such as USB, email, network, print etc.)

13. Implement data labelling solution for classifying all unstructured data based on the data classification policy
14. Data Disclosure, sharing, exchange with internal / external stakeholders and government / public agencies / legal requirements.
15. Data infringement reporting and mechanism

Deliverables

- Data Governance Framework
- Data Classification Policy, Procedures, Templates and Guidelines
- Records Management Policy, Procedures, Templates and Guidelines
- Secure Data Handling Policy & Procedures
- Data Workflow Assessment Report
- Data Risk Assessment Report
- Data Labelling Product & Implementation Support
- Data Disclosure related guidelines / report.

II.B.10. Mobile Application Protection

Identify and verify the mobile application security vulnerabilities against industry global standards such as OWASP, PCI compliance, RBI, MPFI etc.

Scope of Work for Mobile Application Protection

- Perform assessments to identify vulnerabilities that can be exploited using applications on mobile phones for both registered and anonymous users
- Understand the features, functions in the application
- Create a detailed threat profile and a test plan
- Perform automated and manual tests like HTML Source Code Analysis, SQL Injection, Session Hijacking & handling, Cookies, LDAP Injection, Authentication Bypass, security of in-app database etc.
- Secured Network and Application Architecture review of setup deployed for mobile application and its parent web application (if integrated together e.g. internet browser based HRMS and MyHRMS mobile app)
- Assess adequacy, generation & availability of Reports for accounting, regulatory, statutory, reconciliation, MIS & statistical purpose covering all Mobile banking transactions
- Code obfuscation and reverse engineering
- Check Adherence to Operational/Statutory guidelines issued by RBI & other Regulatory bodies w.r.t Mobile Banking Application
- Perform audit of various functionalities provided in the application like Profile Management, Fund transfer, Transactions & queries, Cheque Book related etc.
- Perform verification of the detailed security procedures & processes of the Mobile Banking Solution provider as a part of the existing operational rules & regulations covering transaction, Data & Operational Security setup & establishing the adequacy of the same w.r.t the current Setup.
- Check adequacy of Operational Security features through Access Control, User Rights, Logging, Data integrity, Accountability, Auditability etc. for the Mobile Application Solution

- Check adequacy of MPIN Management Controls (Generation, Re-generation, Authorization, Verifications etc.) of Mobile Banking & Key Management features.
- Conduct audit of various security features including but not limited to Handset Security features, Transaction level security features, Platform Security & reliability features including Database, Network & transmission Security features, Registration features, Administration Portal features, Call logging, tracking & Dispute Resolution features etc.
- Perform analysis/Verification of Audit Logs /Audit Trails of Transactions, Exception List, Non-repudiation violations, Incident management report etc.
- Conduct Digital Forensic Readiness Assessment (DFRA)
- Verify correctness and completeness of integration with SOC, WAF, Firewalls, IPS, AV, AD / DSS, SSO, PIMS, ITAM, DLP, ACC-FIM etc.

Deliverables

The mobile application security report should contain the following at minimum:

- Vulnerabilities identified
- Vulnerability ratings
- Threat Profile
- Test Plan
- Compliance requirements where applicable
- Screenshots and code listing or line numbers where feasible
- Solutions with details and additional resources.

II.B.11. Forensic Analysis

The vendor should be able deploy personnel who can conduct forensic analysis on demand basis and help bank to conduct forensic analysis activities

Scope of Work for Forensic Analysis

The ISSP should have skillset to handle the forensic analysis activities across various IT systems, applications and infrastructure systems in the bank.

ISSP should conduct the activity in a structured fashion using global best practices for conducting forensic analysis. Methodologies and tools should be handled by the vendor for handling the forensic analysis

ISSP should have defined process for the management of the evidences that are collected during the forensic analysis.

Deliverables

Deliverables should include detailed analysis reports, summary reports, evidences collected in scientific manner, etc as required in forensic analysis activity in such a manner that it is producible on any legal/regulatory forum by Bank, with assurance of non-repudiation, audit trail evidences, required by forensic best practices. The forensic report should be admissible as per the domestic and foreign legal framework.

II.B.12. PCI-DSS Services

Scope of Work for PCI DSS

Ensure compliance to the following PCI DSS standard requirements:

- Build and Maintain a Secure Network
  - Setup secure processes for managing security devices including firewalls
  - Implement the process for secure commissioning of servers, network devices, security devices and applications
- Protect Cardholder Data
  - Implement controls to mitigate the risks to card holder data
  - Implement encryption across links including WAN, Internet to protect card holder data
- Maintain a Vulnerability Management Program
  - Setup processes for antivirus management
  - Develop and maintain secure systems and applications
- Implement Strong Access Control Measures
  - Implement controls for authorization and authentication
- Regularly Monitor and Test Networks
  - Implement controls for tracking and monitoring all access to network resources and cardholder data
  - Implement controls to enable periodic testing of IT infrastructure including wireless, applications
- Maintain an Information Security Policy
  - Define policies and procedures that addresses information security for employees and contractors
- Guidance on PCI DSS compliance
  - Provide guidance to implement controls and best practices to achieve compliance.

Deliverables

- Card Holder Data Matrix
- Card Holder Data Flow Diagram
- Card Data Discovery Report
- PCI-DSS Awareness workshop
- Gap Analysis Report
- Vulnerability Scanning Report
- Redesigned – Suggested network Architecture Diagram
- Enhanced Security Policies and Procedures
- Technology evaluation & recommendations
- Sample Security Configuration Assessment Reports
- Network Assessment Report
- Report on Compliance
- Card Brands (Visa) Reporting Documents

II.B.13. ISO 27001 Consulting

SBI currently has some of its units & locations certified on ISO 27001. To advance the maturity levels further, SBI wants to develop detailed Information Security

Management System which is focussed on the on-going management of information security requirements. The intent of the ISMS in SBI is to define the processes requirement to ensure that risks are identified, apprised to management and addressed in an effective manner.

The key components that need to be put in place as that part of ISMS include

- Risk identification and mitigation planning
- Allocation of responsibility for mitigation
- Status tracking of mitigation
- Management reporting
- Security maturity evaluation over a period

Scope of Work for ISMS

1 Define ISMS Structure and roles and responsibilities.
2 Identify a risk assessment methodology that is suited to the ISMS, and the identified business information security, legal, statutory and regulatory requirements.
3 Discuss with the stakeholders and develop criteria for accepting risks and identify the acceptable levels of risk.
4 Interact with key stakeholders and identify all information assets like software assets, databases, records, physical assets, process and service assets, people assets and so on
5 Evaluate the value of the assets based on business impact after detailed discussions with the stakeholders.
6 Perform Risk Assessment by categorizing the assets by profiling threats, assessing vulnerabilities, analysing impact, and ranking/ prioritizing risks based on the level of threat, level of vulnerability and asset value.
7 Analyse and evaluate the risks based on its business impacts, realistic likelihood of security failures, level of risk and the risk acceptance criteria.
8 Identify and evaluate options for the treatment of risks
9 Select control objectives and controls for the treatment of risks
10 Present proposed residual risks to management and obtain their buy-in for implementing and operating ISMS
11 Prepare a Statement of Applicability document
12 Assist in implementing security controls (network architecture, access control systems, and secure configuration guidelines etc.).
13 Assist in defining roles and responsibilities of the enforcer, enabler, and auditor; and establish a total compliance program
14 Conduct internal audits with a trained and appropriately certified team; drawing up performance metrics; conducting awareness programs among end users; defining processes, roles and responsibilities; ensuring that the Management reviews and works on the Action Plan to close non- conformities (NCs).
15 Develop a framework for periodic risk assessment and mitigation; continual user and IT administrator awareness sessions;
16 Develop a framework for security effectiveness measurement and maintenance of dashboards.

Deliverables

- Asset register

- Risk Assessment and Treatment Report
- SOA Document
- Risk Assessment Procedure
- Internal Audit Procedure
- CAPA Procedure
- Effective measurement Metrics
- Effective Measurement Procedure
- ISMS Manual
- Document Control Procedure
- Record Control Procedure
- ISMS Scope
- ISMS Manual
- User Awareness Training presentation
- Quiz Questions & Answers
- Internal Audit Report

II.B.14. ISO 20000

The primary objective of this activity is to implement and certify IT Services Management (ITSM / SMS) for defined scope of work.

Scope of Work for ISO 20000 certification

1. Develop and Implement IT Services Management (ITSM) and obtain ISO 20000 certification for Bank.
   - Baseline the current Services and the IT infrastructure
   - Assess any existing processes against the defined ISO 20000 processes
   - Compare these to business needs and best practices
   - Define and document the ITSM governance principles and policies
   - Design IT Service Management System (ITSM System) by performing the following activities:
     - Define Goals for Service Management & Metrics
     - Identify Services to create IT Service Catalogue
     - Identify Infrastructure
     - Define Roles and Responsibilities
     - Define IT Service Management Processes
     - Identify tools that can aid automation
   - Assess the continuity capabilities of IT infrastructure and processes and define approaches to resume critical activities
   - Assist the identified coordinators to implement and operationalize ITSM processes through trainings
   - Conduct internal audit in line with ITSM implementation requirements
   - Support the internal teams with coordination for certification audit
2. The ITSM should be designed in a manner to enable the effective co-existence of any existing standards like ISO9001: Quality Management System (QMS) and ISO27001: Information Security Management System (ISMS)
3. The implementation must consider improving process maturity level, introducing any needed process required to fulfil the requirement and provide all necessary deliverables related to it.
4. Provide any needed tool/SW to achieve the ISO20000 certification.

Deliverables

- Proposed ITSM System including
  - Policies, Procedures and Guidelines
  - Structure
  - Metrics Reporting Framework
- IT Service Catalogue
- Service Management Plans & SLA Templates
- Updated Service Level Agreements
- Tool Recommendations
- High level strategy and plan for review of critical systems
- Internal Audit report
- Corrective & Preventive Action Plans

Other Deliverables:

- Carrying out security risk assessments of applications, API, Web, Database, Middleware.

- Carrying out security risk assessments of the Network architecture, design, Firewalls, IPS, Wi-Fi, VPN etc.

- Assessments of Infrastructure & data security related areas of Active Directory, Email security, DNS, Proxy, Data security (DLP, DRM),

- Implementation of Information security projects as and when they come up.

The Vendor should comply with Bank's IS Security policy in key concern areas relevant to the RFP. Some of the key areas are as under:

- Responsibilities for data and application privacy and confidentiality
- Responsibilities on system and software access control and administration
- Custodial responsibilities for data, software, hardware and other assets of the Bank being managed by or assigned to the Vendor
- Physical Security of the facilities
- Physical and logical separation from other customers of the Vendor
- Incident response and reporting procedures
- Password Policy of the Bank
- Data Encryption/Protection requirement of the Bank

Appendix-C

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

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

Annexure A

Details of the Bidder

1. Name of the bidder –
2. Date of Incorporation and / or commencement of business in India
3. Certificate of incorporation in India
4. GSTN details
5. Brief description of the Bidder including details of its main line of business
6. Company website URL
7. Details of 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

Seal of Company

Annexure B

Eligibility Criteria

Bidders meeting the following criteria are eligible to submit their Bids along with supporting documents. If the Bid is not accompanied by all the required documents supporting eligibility criteria, the same would be rejected:

Sr. No.	Eligibility Criteria	Documents to be submitted
1.	The bidders must be an Indian firm/ organization/ company registered under Companies Act, empanelled by CERT-In as Information Security Auditing Organisations.	Copy of the Certificate of Incorporation issued by Registrar of Companies and full address of the registered office Or Firm registration certificate along with documents in respect of incorporation with full address of the firm. Current Empanelment Certificate by CERT-In
2.	Bidders should have reported net profit in 2 years out of last 3 financial years (2020-21,2021-22 & 2022-23).	Copy of the audited Balance Sheet
3.	Bidders should have average turnover of Rs. 5 (Five) Crores for the last three financial years (2020-21,2021-22 & 2022-23) from Information Security Services.	Copy of the audited balance sheet
4	Experience and expertise in carrying out security assessments of applications, API, Web, Database, Middleware **(from Domestic/Global BFSI segment of last 3 years (from 01.04.2021 to 31.03.2024) annual average aggregate value of work orders should be minimum 1.00 Crore from at least 5 clients).**	Copies of work orders
5	Experience in carrying out security risk assessments of the Network architecture, design, Firewalls, IPS, Wi-Fi, VPN etc. Experience and expertise in Infrastructure & data security related areas of Active Directory, Email security, DNS, Proxy, Network Security, Cloud Security, Data security (DLP, DRM), Experience in implementing Information security projects as and when they come up. The Bidders should have a pool of minimum 200 full time professionals with requisite skills and experience.	1. Please provide exact numbers of certified officials from the mentioned domains. 2. Please attach sample resumes of twenty (20) team members from the mentioned domains.

6	The Bidder should not have been blacklisted / debarred by any Government / Government Organisation / PSU / PSB / IBA / RBI / SEBI / Regulatory bodies for Information and Cyber Security Audit and Security review.	Self-Certification

Annexure C

Technical Bid

Sl. No	Activities related to Information Security	Weightage %	Details required in Annexure
1	Indian & Global clients' assignments handled	20	C1
2	Skilled personnel resources available	15	C2
3	Technical skills & Credentials (tools created, R&D work done, papers/journals published, forensics assignments done)	5	C3
4	Depth & Breadth of information security assignments handled. Credentials / certifications etc. Committee membership in Govt / RBI /IDRBT / Cert-IN / Gartner etc.	30	C4 & C5 & C6
5	Presentation to TPNC committee	20	C7
6	Client feedback of two (2) clients of national/international repute as provided in point 1 in this table	10	
		100	

- Bidders to provide required details as per Annexure C1 to C6 for Sl.No.1 to 4 above.
- Details should be related to the period 2020 – 2023.
- Supporting documents for above should be Purchase / Work Orders, letters from clients on their letter head, contacts of clients etc.
- Only such assignments should be described in above table which are directly related to Scope of Work of this RFP

Signature

Seal of Company

Annexure C1

Experience about Domestic & Global Clients

For the period April 2020 to March 2023

Amount in INR Lacs

Sr. No.	Particulars	Amount
A1	Name & Billing Amount for Domestic & Global BFSI segment	
A2	Total Billing Amount pertaining to TOP 5 Clients for Domestic & Global BFSI segment	
B1	Total Billing Amount for Domestic & Global non-BFSI Segment	
	TOTAL	

Please Note:

- Supporting documents for above should be Purchase / Work Orders, letters from clients on their letter head, contacts of clients etc.
- Only such assignments should be described in above table which are directly related to Scope of Work of this RFP

Score (Total Score -20)

S.No	Description	Score
A1 – Billing from Domestic & Global BFSI Segment (A1)		
a	Amt >= 20 crore	15
b	Amt >= 15 crore	12
c	Amt >= 10 crore	10
d	Amt >= 5 crore	6
e	Amt >= 1 crore	3
A2 – Billing from Top 5 Clients		
a	Amt >= 8 crore	5
b	Amt >= 5 crore	3
c	Amt >= 1 crore	1

Signature

Seal of Company

Annexure C2

Skilled personnel resources available

Security Review Area	Count of present Resources Level Wise	No. of resources can be engaged on-site in Mumbai (within 15 days of PO)	No. of resources can be engaged on-site in Mumbai (within 30 days of PO)
Total Unique Resources presently with Bidder	**L1 – L2 – L3 – L4 -**	**L1 – L2 – L3 – L4 -**	**L1 – L2 – L3 – L4 -**

Activity wise Resources wise information is required to fill in annexed excel sheet.

Please Note:

- The details should be related to the resources who are posted in Mumbai/ Navi Mumbai and willing to work in Mumbai/Navi Mumbai only. (Details has to be provide in 'Resource Details' sheet of attached excel sheet – ' RFP for ISSP empanelment 2024-27'

- Preference will be given to the bidder who has experienced resources in all below areas.

Score (Total Score -15)

S.No	Description	Score
1. L1 Resources		
a	count of L1 resources > 20	4
b	count of L1 resources > 15	3
c	count of L1 resources > 10	2
d	count of L1 resources > 5	1
2. L2 Resources		
a	count of L2 resources > 40	5
b	count of L2 resources > 30	4
c	count of L2 resources > 20	3
d	count of L2 resources > 10	2
e	count of L2 resources > 5	1
3. L3 Resources		
a	count of L3 resources > 10	4
b	count of L3 resources > 8	3
c	count of L3 resources > 5	2

d	count of L3 resources > 2	1
4. **L4 Resources**		
a	count of L4 resources > 3	2
b	count of L4 resources > 1	1

Signature

Seal of Company

Annexure C3

Organisation Skill: Technical Skills and Credentials

For the period April 2020 to March 2023

Sl. No	**Particulars of the activity**	**No. of Clients where it is used/activity performed**	**Year of activity**	**Score Pattern (Total Score -5)**
A. Tools Created				Score '1' for proprietary tool created and used else '0'
B. Framework Created				Score '1' for framework created related to Information Security activities else '0'
C. Paper/Journals Published				Score '1' for Paper/Journals Published in national/international forums related to Information Security activities else '0'
D. Forensic Assignment				Score 2 for forensic assignment > 3, Score 1 for forensic assignment > 1,

Score (Total Score -5)

Please Note:

- Supporting documents for above should be Purchase / Work Orders, letters from clients on their letter head, contacts of clients etc.
- Only such assignments should be described in above table which are directly related to Scope of Work of this RFP

Signature

Seal of Company

Annexure C4

Depth & Breadth of information security assignments

For the period April 2020 to March 2023

Amount in INR Lacs

Sl.No.	Domain Area	Experience (Yes / No)	If YES, Billing Amt for individual activity for BFSI clients (Indian / Global)
1	Web Application security Review		
2	Mobile Application Security Review		
3	Compliance audits (ISO 27001, ISO 22301, PCIDSS, etc.)		
4	VAPT & Configuration Testing		
5	Security Architecture Review		
6	Data Protection Compliance Audit/Review (Data Protection Act of India etc.)		
7	Regulatory Information Security Audit/Review (Aadhaar (AUA , Sub-AUA etc.) , RBI, IRDAI etc.)		
8	Competence to Review New IT areas like cloud, IOT, AI/ML etc		
9	Thematic security Audits		
10	Cyber Security Posture Assessment		
	TOTAL		

Score (Total Score -20)

Please Note:

- Supporting documents for above should be Purchase / Work Orders, letters from clients on their letter head, contacts of clients etc.
- Only such assignments should be described in above table which are directly related to Scope of Work of this RFP

Signature
Seal of Company

Annexure C5

Certifications/Accreditations/Awards

For the period April 2020 to March 2023

Sl. No.	Particulars	Awarded by	Scoring Patterns
1	Accreditations/Certifications		Score 1, if Bidder has got accreditation/certified from Indian /global bodies other than CERT-In
2	National & International Awards		Score 1, if Bidder has got distinctive award from Indian /global bodies
3	Committee member Govt/PSU/Intl Forum		Score 2, if Bidder is core member on at least 3 national/international forums Score 1, if Bidder is core member on at least 1 national/international forums
4	Gartner		Score 1, if Bidder has got Gartner distinctive position by Gartner

Score (Total Score -5)

Please Note:

- Supporting documents for above should be nominations/certifications/documents etc.
- Only such testimonials should be described in above table which are directly related to Scope of Work of this RFP

Signature

Seal of Company

Annexure C6

Specialized/emerging threat handling capacity of the bidder

For the period April 2020 to March 2023

List of activities (like Cyber Forensics/Digital Forensic/Red Teaming/Tabletop Exercise/ / Threat modelling and Digital Forensic readiness etc.) carried out by the bidders.

Sl.No.	Name of the customer/firms	Type of activity	Tools used	Description of the activity	Period From date – To Date
					2020-2023

Please Note:

- Supporting documents for above should be Purchase / Work Orders, letters from clients on their letter head, contacts of clients etc.
- Only such assignments should be described in above table which are directly related to Scope of Work of this RFP

Score (Total Score -5)

S.No	Description	Score
a	activities > 20	5
b	activities > 15	4
c	activities > 10	3
d	activities > 5	2
e	activities > 1	1

Signature

Seal of Company

Annexure C7

Statement of the Bidder

For the period April 2020 to March 2023

Sl. No	Name, Address & Contact details of CIO/CISO/Senior Management	Particulars of the order	Month & year of order	Description of services (relevant to Scope of Work in this RFP, give reference number only)	Domestic/Foreign	Value of order in INR	Duration of engagement	Date of completion (as per contract)	Date of completion (actual)	Remarks for extended completion, if any
A. Scheduled Commercial Banks										
1.										
2.										
B. NBFCs										
1.										
2,										
C. Private Companies										
1.										
2.										
D. Govt Companies/PSUs										
1.										
2.										

- Assignments done during the financial years 2020 to 2023 should only be described as per Annexure C1 & C2
- Supporting documents should be Work Orders, letters from clients on their letter head, contacts of clients etc., should be enclosed. Only such assignments should be described in above table which are directly related to Scope of Work of this RFP.
- Brochures / emails attached shall not be considered for evaluation.

Documentary evidence must be furnished against each of the above criteria along with an index. All documents must be signed by the authorized signatory of the bidder. Relevant portions, in the documents submitted in pursuance of eligibility criteria, should be highlighted. Misrepresentation discovered, at any stage, may result into disqualification of the bidder from empanelment process.

Signature

Seal of Company

Annexure C8

Preferred Activities by ISSP

Sl. No.	Standardized Services	Have capability (Y/N)	If Yes in previous col. Indicate priority of interest levels in offering this service to Bank (1 is Top Priority)	Remarks
1	Vulnerability Assessment			
2	Penetration testing			
3	Technical standard creation			
4	General Process Review			
5	IT General Controls Review			
6	ISO 27001 ,ISO 22301Consulting			
7	Vendor Risk Assessment			
	Specialized Services			
8	IS Program Management			
9	Log Monitoring			
10	Information Security Awareness			
11	Application Security			
12	Code Review			
13	Domain/Channel Process Review			
14	BCP / DRP			
15	Security solution consulting			
16	Product evaluation			
17	Data Governance			
18	Mobile Application Protection			
19	Forensic Analysis			
20	PCI-DSS Services			
21	ISO 20000			

Annexure D - Non-Disclosure Agreement

THIS RECIPROCAL NON-DISCLOSURE AGREEMENT (the "Agreement") is made at *Mumbai* between:
_____ constituted under the _____ Act, _____ having its Corporate Centre at _____ _____ (hereinafter referred to as "Bank" which expression includes its successors and assigns) of the ONE PART;

And
_____ (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. 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 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 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; or (iv) is independently developed by Receiving Party.

(c) "Confidential Materials" shall mean all tangible materials containing Confidential Information, including without limitation, email, 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 own employees and other persons and then only to those employees and persons 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 its employees and consultants specifically assigned and/or otherwise, sufficient to enable it to comply with all the provisions of this Agreement. If the Contractor shall appoint any Sub-Contractor then the Contractor may disclose confidential information to such Sub-Contractor subject to such Sub Contractor giving the Customer an undertaking in similar terms to the provisions of this clause.

(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 prior to such disclosure and shall comply with any applicable protective order or equivalent. The intended recipients for this purpose are:

(1) the statutory auditors of the Customer and

(2) regulatory authorities regulating the affairs of the Customer and inspectors and supervisory bodies thereof

(c) The foregoing obligations as to confidentiality shall survive any termination of this Agreement as also dissolution of the company/bidder where the partners/directors would continue to be responsible for the said confidentiality.

(d) 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 to prevent mixing.

(e) Receiving Party may not reverse engineer, decompile or disassemble any software disclosed to Receiving Party.

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 (as listed below), to injunctive or equitable relief as may be deemed proper by a Court of competent jurisdiction.

a. Suspension of access privileges
b. Change of personnel assigned to the job
c. Financial liability for actual, consequential or incidental damages
d. 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 property 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 patents, copyrights, trademarks, or trade secret information.

(b) Any software and documentation provided under this Agreement is provided with RESTRICTED RIGHTS.

(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 Indian Arbitration and Conciliation Act 1996 or any Amendments or Re-enactments thereto.

(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) All obligations created by this Agreement shall survive change or termination of the parties' business relationship.

5. Suggestions and Feedback

(a) 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 party 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 _____*2024* at _____
(month) (place)

For and on behalf of _____

Name		
Designation		
Place		
Signature		

For and on behalf of _____

Name		
Designation		
Place		
Signature		

Annexure E - Compliance Statement

Declaration

Terms & Conditions

We hereby undertake and agree to abide by all the terms and conditions stipulated by the bank in the RFP document.

We certify that the services offered by us in response to the bid conform to the technical specifications stipulated in the bid with the following deviations:

1)
2)
….

(If left blank it will be construed that there is no deviation from the specification given above)

Signature:

Seal of Company

Annexure F

Commercial Bid

The commercial Bid needs to contain the information listed hereunder bearing the identification – "Commercial Bid for Empanelment of Information Security Service Providers (ISSPs)".

Name of the Bidder: Level 1 Experience of 1 year and up to 4 years	**Educational qualifications:** Graduation in CS or IT or Information Security or Cyber Security • Mandatory Certifications: CEH/LPT/ISO 27001 LA/LI • Experience: Having good experience in application & Infrastructure security assignments. Have done IS assessments OR IS systems/solution management.
Level 2 Experience of above 4 years and up to 8 years	**Educational qualifications:** Graduation in CS or IT or Information Security or Cyber Security • Mandatory certifications: CISA/CISM/CISSP/OSCP/ Infrastructure security solution certifications. • Experience: In carrying out security assessments. Excellent knowledge in security solutions and technologies. Banking domain knowledge will be added advantage.
Level 3 Experience of above 8 years and up to 12 years	**Educational qualifications:** Education Graduation in CS or IT or Information Security or Cyber Security • Mandatory certifications: CISA/CISM/CISSP/OSCP/ OSCE (Minimum two) / Infrastructure security solution certifications. • Experience: excellent domain knowledge in application or infrastructure management / assessments. Banking domain knowledge will be added advantage.

Level 4 Experience above 12 years	**Educational qualifications:** Graduation in CS or IT or Information Security or Cyber Security • Mandatory certifications: CISA and two of CISSP/OSCP/OSCE/CEH/ Infrastructure security solution certifications. • Experience: excellent domain knowledge in application or infrastructure management / assessments. Banking domain knowledge will be added advantage.

Sr. No.	Resource Level	Resource Cost per person /per day (Rs.)	Resource Cost per person / per month (Rs.) (if retained for a minimum duration of one month for a regular routine)
1.	L-1		
2.	L-2	**1.42 Times of L-1**	**1.42 Times of L-1**
3.	L-3	**1.73 Times of L-1**	**1.73 Times of L-1**
4	L-4	**2.55 Times of L-1**	**2.55 Times of L-1**
…			

Item	% increase over original rate agreed (for new assignments ordered during a year.	Remarks
Yearly step-up		

Outstation Travel – Out of Pocket / Lodging /Boarding expenses – on actuals subject to a maximum of Rs. 4000 /-per day.

Air Travel – Economy class lowest fare **from**
Company's head office /
Mumbai/
current location of resource

whichever is lowest

to the activity location

Note: The quoted prices shall be exclusive of all taxes and statutory levies such as Service Tax/VAT, Sales Tax etc.

All taxes & statutory levies should be specified explicitly.

Signature

Seal of Company

------- End of Document -------