GeM Bid Ref: GEM/2025/B/6707442 **Date:** ***20.09.2025***

REQUEST FOR PROPOSAL (RFP)

FOR

Selection and Appointment of service provider for Incident Response (IR), Cyber/Digital forensic services, Red Team, Tabletop & Cyber Drill Exercise

RFP Reference No.	***GEM/2025/B/6707442***
RFP Issuance Date	***20.09.2025***
Last Date of request for Queries/ Clarifications	***25.09.2025***
Date and time of Pre-Bid Meeting	***26.09.2025 03:00PM***
Last Date for receipt of bids	***13.10.2025 03:00PM***
Date and time of opening Technical bids	***13.10.2025 03:30PM***

Issued by:

Information System Security Department
Ground Floor, 66, Rajaji Salai, Chennai – 600 001
Phone: 044-25279728
Email: *arvind.kumar@indianbank.co.in, anil.lakra@indianbank.co.in*
Website: https://www.indianbank.bank.in

	3. Authorization to Bid
	4. Timeframe for completion of activities
	5. Payment Terms
	6. Service Level Agreement (SLA)
	7. Contract Period
	8. Sub-Contracting
	9. Governing language
	10. Insurance
	11. Jurisdiction and Applicable Law
	12. Liquidated Damages (LD)
	13. Bank's right to accept or reject any bid or all bids
	14. Performance Security
	15. Limitation of Liability
	16. Indemnity Clause
	17. Disclaimer
	18. Patent Rights
	19. IT Act 2000
	20. Intellectual Property Rights (IPR)
	21. Acceptance of Purchase Order
	22. Signing of Contract Form, NDA, SLA and Submission of Undertaking of Labour Law Compliance
	23. Settlement of Disputes
	24. Exit Requirements
	25. Termination for Convenience
	26. Termination for Default
	27. Force Majeure
	28. Termination of Services/ Contract
	29. Confidentiality
	30. Negligence
	31. Amalgamation
	32. Software/Hardware requirements

Annexure – VI	Non-Disclosure Agreement
Annexure – VII	Declaration for MSME benefits
Annexure – VIII	Declaration on Procurement from a bidder of a country which shares a land border with India
Annexure – IX	Certificate of local content as per Make in India guidelines
Annexure – X	Undertaking for Labour Law Compliance
Annexure - XI	Pre-Bid Query Format
Annexure - XII	Experience Details of the Bidder/OEM
Annexure – XIII	Turnover, Net Worth and P&L Details
Annexure – XIV	Bid Security Form
Annexure – XV	Manufacturers' Authorization Form
Annexure – XVI	Undertaking of Authenticity
Annexure – XVII	Client References
Annexure – XVIII	Software Bill of Materials (SBOM)
Annexure - XIX	Checklist for the RFP
Annexure - XX	Service Level Agreement

GeM Bid Ref: GEM/2025/B/6707442 **Date:** ***20.09.2025***

SCHEDULE [A]: IMPORTANT DATES AND INFORMATION ON RFP SUBMISSION

S. No	Particulars	Timeline
1	**Issuance Date of RFP** (Date of RFP Issuance)	20.09.2025
2	**Last Date of request for Queries/ Clarifications** (Last Date of Receiving request for queries / clarifications before the Pre-bid Meeting)	25.09.2025 Format for seeking clarification is enclosed as Annexure-XI
3	Pre–bid Meeting Date and Venue Details	26.09.2025 3:00PM through physical / virtual mode. Bidders willing to participate in pre-bid meeting need to submit their details at arvind.kumar@indianbank.co.in on or before *25.09.2025* Details of virtual/ physical pre-bid meeting would be communicated via e-mail to interested bidders separately.
4	**Last Date of Submission/ Closing Date in Online & Offline Mode** (Last Date of Submission of RFP Response)	13.10.2025 for both online bid and offline document submissions. For Offline submission of documents listed in Sl. No. 8 below, the sealed envelope shall be addressed to the Bank and to be delivered at the address below. Assistant General Manager, Indian Bank, Head Office, ISSD Department, Ground Floor, 66, Rajaji Salai, Chennai - 600001
5	**Eligibility cum Technical Bid Opening Date**	13.10.2025 03:30 PM
6	**Reverse Auction**	The commercial bids submitted by the bidders will be opened as per GeM terms and the reverse auction will be conducted among those bidders who satisfy the eligibility criteria and qualify in technical evaluation. Further H1 elimination may

		be done as per the GeM guidelines defined in the GeM Bid Document.
7	**Online Bid Submission Details**	This RFP will follow e-Procurement (e-Tendering) process and the same will be conducted through Government e-Market Place (GeM) portal. The documents listed below in Sl.No 8 only to be submitted in offline physical mode.
8	**Documents to be submitted physically by Bidders** **(Offline Mode)**	1. Bid Security (EMD) for Rs.15,00,000/- to be submitted in the form of DD/ Fund transfer/ Bank Guarantee (issued by a nationalised/ scheduled commercial Bank located in India (other than Indian Bank) in favour of "Indian Bank" payable at Chennai. BG should be valid for 225 days from the last date for submission of the Bid (in the format provided at annexure XIV) (or) Fund transfer to be made in the account as detailed under: Account No.: 743848138 Account Name: INDIAN BANK, H.O. TECHNOLOGY MANAGEMENT DEPARTMENT-II IFSC Code: IDIB000H003 Branch: Harbour 2. Pre-Contract Integrity Pact (on stamp paper)
9	**RFP Coordinators**	1. Shri. Arvind Kumar Tel: 044-25278750 e-mail: arvind.kumar@indianbank.co.in 2. Shri. Anil Kumar Lakra Tel: 044-25279728 e-mail: anil.lakra@indianbank.co.in 3. Shri Rikesh Ramakant Shah e-mail: Rikesh.Shah@indianbank.co.in 4. Shri. Sreehari T Tel: 044-25279732 e-mail: sreehari.t@indianbank.co.in
The RFP document can also be downloaded from: **Bank's website: https://www.indianbank.bank.in and**		

Government e- Market Place (GeM) portal

In addition to above, a paper publication will be made for the information to the prospective bidders regarding this RFP. However, clarifications, modifications and date of extensions, if any, will be published in the Bank's website and GeM portal only.

I. Note: Indian Bank, does not take responsibility of any bid/offer damaged/lost in transit/delivered at incorrect address prior to its receipt at the Bank's designated office.

II. Bank will follow two bidding system. Part-I (Technical Bid) of the bid contains compliance details of the eligibility and terms & conditions set in the RFP document (including annexures) for which proposal/quotation is called for. Bids have to be submitted in **online mode only** through **Government e- Market Place (GeM) portal** along with physical submission of certain documents at designated office as mentioned in Point No. 4 of Schedule [A] (Important Dates and Information on RFP Submission). Further, Bidders must submit their commercial bid as per the format given in the RFP (as per Part-II of Section-V) along with the technical bid on the e-procurement (GeM) portal. Technical bids submitted by all the bidders will be evaluated and only technically qualified bidders will be called for opening of commercial bids.

1. Bidders should enrol/ register themselves on Government e- Market Place (GeM) portal before participating in bidding. All the documents in support of eligibility criteria etc. are also to be scanned and uploaded along with the tender documents. Except as provided in this RFP, any document sent by any other mode will not be accepted.

2. Documents which are to be uploaded online are required to be duly signed by the Authorized Signatory under the seal of the bidder company/ firm in every page. Any correction should be authenticated by the same signatory. If insufficient or false information is furnished and/or if there is any deviation or non-compliance of the stipulated terms and conditions, the bid will be liable for rejection.

3. The price quoted should be unconditional and should not contain any string attached thereto. Bid, which do not confirm to our eligibility criteria and terms & condition, will be liable for rejection.

III. The RFP document (along with addendums, if any) needs to be signed and stamped by the authorised signatory of Bidder and it must be submitted along with the Technical Bid as an evidence of having read and understood the contents of RFP and its addendums(if any).

IV. Time wherever mentioned in this RFP is as per Indian Standard Time. The above dates and timelines are subject to change with prior notice or intimation. If a holiday is declared on the dates fixed for submission of bids, opening of bids (Technical or

Commercial) or presentation, the same shall stand revised to the next working day at the specified time and place unless communicated otherwise.

This RFP is issued by:

Assistant General Manager
Indian Bank, Head Office,
Information System Security Department,
Ground Floor, 66, Rajaji Salai,
Chennai – 600001

SCHEDULE [B] GLOSSARY OF TERMS

i) Following terms are used in the document interchangeably to mean:

1. Bank refers to "Indian Bank (IB)"' including its Branches, Administrative offices, processing centres/HUBS, cells and all other units and establishments etc. (excluding its overseas establishments and Regional Rural Banks).
2. Recipient, Respondent, Consultant, Consultancy firms, Bidder, Applicant means the respondent to the RFP document.
3. RFP means the "Request for Proposal" document.
4. Proposal, Bid means "Response to the RFP Document".
5. Tender means RFP response documents prepared by the Bidder and submitted to "Indian Bank".
6. Selected bidder and the Bank shall be individually referred to as "party" and collectively as "parties". The terms, Successful bidder and the Bank are also referred as Supplier/ Service provider and Purchaser respectively.
7. The term "Bid" & "Quote/ Quotation" bears the same meaning in this RFP.
8. Unless contrary to the context or meaning thereof, Contract or agreement wherever appearing in this RFP shall mean the contract to be executed between the Bank and the successful bidder.
9. Unless the context otherwise requires, reference to one gender includes a reference to the other, words importing the singular include the plural and words denoting natural persons include artificial legal persons and vice versa.

ii) Other Terms and abbreviations**:**

Sl. No.	Terms used in the RFP	Terms and abbreviations
1	GOI	Government of India
2	RBI	Reserve Bank of India
3	IBA	Indian Banks' Association
4	GFR	General Financial Rules
5	POA	Power of Attorney
6	IMPS	Immediate Payment Service
7	NEFT	National Electronic Funds Transfer
8	RTGS	Real Time Gross Settlement
9	CTS	Cheque Truncation System
10	IEM	Independent External Monitor
11	DPIIT	Department for Promotion of Industry and Internal Trade
12	MSE	Micro and Small Enterprises

13	MSME	Micro, Small & Medium Enterprises
14	LLP	Limited Liability Partnership
15	OEM	Original Equipment Manufacturer
16	EMD	Earnest Money Deposit
17	WCS	Weighted Commercial Score
18	WTS	Weighted Technical Score
19	SOW	Scope of Work
20	TCO	Total Cost of Ownership
21	API	Application Programming Interface
22	PBG	Performance Bank Guarantee
23	CASA	Current Account Savings Account
24	ISO	International Organization for Standardization
25	GST	Goods and Services Tax

Any term used in this document and not specifically defined herein will have the same meaning as provided in relevant RBI regulations and/ or RBI/IBA guidelines and in case of any dispute the decision of the Bank shall be final and binding.

Confidentiality:

This document is meant for the specific use by the Bidder/s to participate in the current tendering process. This document in its entirety is subject to Copyright Laws. Indian Bank expects the Bidders or any person acting on behalf of the Bidders to strictly adhere to the instructions given in the document and maintain confidentiality of information. ***The Bidder/s do hereby undertake that they shall hold the information received by them under this RFP process or the contract "in trust" and they shall maintain utmost confidentiality of such information. The Bidders have to agree and undertake that (a) They shall maintain and use the information only for the purpose as permitted by the Bank (b) To strictly allow disclosure of such information to its employees, agents and representatives on" need to know" basis only and to ensure confidentiality of such information disclosed to them****. The Bidders will be held responsible for any misuse of information contained in this document or obtained from the Bank during course of RFP process, and liable to be prosecuted by the Bank in the event such breach of confidentiality obligation is brought to the notice of the Bank. By downloading the document, the interested parties are subject to confidentiality clauses.*

SCHEDULE [C] DISCLAIMER

The information in this Request for Proposal ("RFP") document provided to bidders or applicants whether verbally or in documentary form by or on behalf of Indian Bank, is under the terms and conditions set out in this RFP document and shall also be subject to all other terms and conditions to which such information is generally made available. This RFP document is not an agreement, offer or an invitation by Indian Bank to enter into an agreement/contract in relation to the service but is meant for providing information to the applicants who intend to submit the bids (hereinafter individually and collectively referred to as "Bidder" or "Bidders" respectively). This RFP is designed with the purpose to assist the applicants/ Bidders to formulate their proposal and does not claim to provide all the information that may be required by the applicants/ Bidders.

Each Bidder may conduct its own independent investigation and analysis and is free to check the accuracy, reliability, and completeness of the information in this RFP. Indian Bank and its directors, officers, employees, respondents, representatives, agents, and advisors make no representation or warranty and shall incur no liability under any law, statute, rules, or regulations as to the accuracy, reliability or completeness of this RFP. The information contained in the RFP document is selective and is subject to updation, expansion, revision, and amendment. It does not purport to contain all the information that a Bidder may require. Indian Bank does not undertake to provide any Bidder with access to any additional information or to update the information in the RFP document or to correct any inaccuracies therein, which may become apparent.

The Bidders, by accepting this document, agree that any information contained herein may be superseded by any subsequent written information on the same subject made available to the bidders or any of their respective officers/ employees or published in the Bank's website and/or GeM portal. It is also understood and agreed by the Bidder/s that decision of the Bank regarding selection of the Bidder will be final and binding on all concerned. No correspondence in this regard, verbal or written, will be entertained.

It shall be the duty and responsibility of the Bidders to ensure about their legal, statutory and regulatory eligibility and other competency, capability, expertise requisite for them to participate in this RFP process and to provide all the services and deliverables under the RFP to the Bank.

The applicant shall bear all its costs associated with or relating to the preparation and submission of its proposal including but not limited to preparation, copying, postage, delivery fees, expenses associated with any demonstrations or presentations which may be required by the Bank or any other costs incurred in connection with or relating to its proposal. The Bank shall not be liable in any manner whatsoever for the same or for any other costs or other expenses incurred by an applicant in preparation or submission of the proposal, regardless of the conduct or outcome of the selection process.

Indian Bank in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP. Such change will be published on the Bank's Website and GeM Portal and it will become part and parcel of RFP.

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

GeM Bid Ref: GEM/2025/B/6707442 **Date:** ***20.09.2025***

SCHEDULE [D] GENERAL INFORMATION

Indian Bank (hereinafter called the "Bank") is floating Request for Proposal (RFP) for Selection and Appointment of service provider for Incident Response (IR), Cyber/Digital forensic services, Red Team, Tabletop & Cyber Drill Exercise for a period of 3 years.

Shortlist of Bidders shall be prepared after evaluation of the technical Bids submitted by the bidders participated in this RFP.

Bidders are hereby advised to carefully review and submit all relevant information in the same chronology under the relevant sections only, with their RFP responses.

Details of the objectives, scope of the services, eligibility and qualification criteria, data & documents required (if any) to be submitted along with RFP. Criteria that would be adopted for evaluation of the responses for short listing and other information is contained in the RFP document.

The RFP document can be downloaded from GeM portal or from the Bank's website www.indianbank.bank.in and alternatively hard copies of the document can be obtained from Indian Bank Head Office, Information System Security Department, Ground Floor, 66 Rajaji Salai, Chennai – 600001, if needed.

GeM Bid Ref: GEM/2025/B/6707442 **Date:** ***20.09.2025***

SCHEDULE [E] OVERVIEW OF INDIAN BANK

Indian Bank, with Corporate Office in Chennai was established as part of the Swadeshi Movement on August 15, 1907.

Along with 13 other banks, the Bank was Nationalized on July 19, 1969. The Bank celebrated its centenary in August 2007. With effect from 1st April 2020, erstwhile Allahabad Bank merged into Indian Bank. The integration of CBS systems of both the banks was completed on 14/02/2021. In the last 115 years, Bank has established a rich legacy by providing quality financial services. It has passed through challenging times, successfully registered turnaround and emerged stronger than before. Given the ever-changing requirements, Bank fine-tuned its strategies and undertook several structural and operational changes and earned a coveted position in the Indian banking industry. Bank's foremost priority has been to serve the people and its nation.

The Bank has been pioneer in developing many digital products and received many awards on digital front.

VISION:

"Delivering excellence in financial services through customer focus, employee engagement and sustainable growth"

MISSION:

- Bring the best of innovation and technology in our offerings
- Be responsive to the unique needs of every customer through all channels of choice
- To provide value to stake holders
- Empower and engage our employee

As on 31st March 2025, Bank's total Global business reached Rs.13.25 Lakh Cr. consisting of Deposits at Rs.7.37 Lakh Cr and Advances at Rs.5.88 Lakh Cr.

As on 31st March 2025 Bank has Pan-India network with 5901 Branches including 3 DBU, 5268 ATMs/BNAs, 14,667 Business Correspondents. The Bank has expanded its footprint overseas with branches at Singapore, Colombo and Jaffna, besides a Foreign Currency Banking Unit in Colombo.

Bank had always been a forerunner in offering digital products which provide hassle free, convenient and safe transaction facilities to enhance customer experience, meeting their expectations as the country gears itself for riding on the digital wave. After the amalgamation, the Bank is poised to grow on both business and profitability fronts. The emphasis will be to leverage operational efficiencies, cost synergies and new opportunities in terms of Brand and reach to deliver enhanced customer experience. The focus will be on increasing the CASA share in deposits while looking at diversified growth in credit. Cost optimisation and increasing revenue with focus on fee income, improving recovery and containing NPAs will be levers to improve bottom line.

Technology Environment

Indian Bank has all its branches on Core Banking Solutions, has a range of customer centric and other solutions like full suite of Core Banking Solution, payment systems like IMPS, NEFT, RTGS, SWIFT, CTS, etc., alternate delivery channels viz., ATM, e-Kiosk, Internet Banking, Mobile Banking, e-payment of Taxes, Utility Bill, Ticket, Donation, etc., SMS alerts and Corporate Net Banking. Bank has launched an integrated mobile app having various functionalities with biometric / face id login.

As a part of enhancing customer experience, Bank has also launched an AI-Chatbot ADYA, that is currently available on Bank's website and Mobile Banking App as an additional interface for answering customer queries and lead generation.

For further details, please visit Bank's website www.indianbank.bank.in

GeM Bid Ref: GEM/2025/B/6707442 **Date:** ***20.09.2025***

SECTION – I

REQUEST FOR PROPOSAL (RFP)

Indian Bank is a Public Sector Bank, headquartered at Chennai. The Bank has Pan-India network with 5901 Branches including 3 Digital Banking Units, 5268 ATMs/BNAs, 14,667 Business Correspondents and serves over 100 million customers. The Bank has expanded its footprint overseas with branches at Singapore, Colombo and Jaffna, besides a Foreign Currency Banking Unit in Colombo. As on 31st March 2025, Bank's total Global business reached Rs. 13.25 Lakh Cr consisting of Deposits at Rs.7.37 Lakh Cr and Advances at Rs.5.88 Lakh Crores.

Bank's Information Systems and Security processes are certified with ISO27001:2013 standard and is among very few Banks certified worldwide. It has overseas branches in Colombo, Jaffna and Singapore including a Foreign Currency Banking Unit at Colombo and an offshore banking unit in Gift City. Post-merger with Allahabad Bank, Indian Bank is the seventh largest bank in the country.

In connection to this, Bank invites sealed offers ('Eligibility cum Technical Proposal/ Bid' and 'Commercial Proposal/ Bid') for selection of service provider as per Bank's requirement and in compliance with the Terms & Conditions, Specifications and Scope of Work described in this document.

The RFP document is not a recommendation, offer or invitation to enter a contract, agreement or any other arrangement, in respect of the supply and services. The provision of the supply and services is subject to observance of selection process and appropriate documentation being agreed between Bank and the successful bidder as identified by the Bank, after completion of the selection process as detailed in this document. This RFP is not transferable. Only the bidder who has submitted the bid will be eligible for participation in the evaluation process.

The Bank is interested in identifying vendor for Incident Response (IR), Cyber/Digital forensic services, Red Team, Tabletop & Cyber Drill Exercise for a period of 3 years.

Bank will follow two bidding system. Part-I of the bid contains compliance details of the specifications for which quotation is called for. The Bidders should enrol/ register themselves on GeM portal before participating in bidding. Except for the documents required to be submitted in physical form to the Bank, Bids have to be submitted online only through GeM portal. The bidders also need to submit necessary documents physically as per RFP through offline mode to the address mentioned in the RFP. The Commercial Bid (Part II) will be submitted separately along with the bid document.

Interested eligible bidders may submit their quotation for providing Selection and Appointment of service provider for Incident Response (IR), Cyber/Digital forensic services, Red Team, Tabletop & Cyber Drill Exercise for a period of 3 years, as specified in Part-I as per the following procedure:

GeM Bid Ref: GEM/2025/B/6707442 **Date:** ***20.09.2025***

1. Bidders should apply through GeM Portal only. All the documents in support of eligibility criteria, technical specifications, annexures etc. are also to be scanned and uploaded along with the tender documents. Bid Documents submitted/sent by any other mode will not be accepted.

2. **Part-I** contains compliance details of the specifications for which Bid is called for. No column shall be left blank or altered.

3. **Part-II** – Commercial along with price break up details to be submitted separately along with the bid documentation (Closed bidding process). After technical evaluation, intimation will be given to all qualifying bidders about the date and time of reverse auction through email alert from GeM.

4. Part-I (as per Section-V - Technical & Functional Specifications) & Part-II (as per Section-V - Commercial bid) to be uploaded online duly signed by the Authorized Signatory under the seal of the bidder company/ firm in every page. The bidders also need to submit necessary documents physically through offline mode to the address mentioned in the RFP. Any correction should be authenticated by the same signatory. If insufficient or false information is furnished and/or if there is any deviation or non-compliance of the stipulated terms and conditions, the quotations will be liable for rejection. The price quoted in the Commercial bid should be unconditional and should not contain any strings attached thereto. The bids which do not conform to our specifications will be liable for rejection and offers with a higher configuration will not attract any special consideration in deciding the vendor.

5. Bank has the right to accept or reject any quotation/cancel the e-tender at its sole discretion, at any point, without assigning any reason thereof. Also, Bank has the discretion for amendment / alteration / extension before the last date of receipt of bid.

6. **MAKE IN INDIA**

This RFP is further governed by Government of India, Ministry of Commerce and Industry, Department of Industrial Policy and Promotion order number P-45021/ 2/2017-B.E.-II dated 15th June 2017 for the Public Procurement (Preference to Make in India), Order 2017, revision order no. P-45021/ 2/2017-PP (B.E.-II) dated 28th May 2018, revision order no. P-45021/ 2/2017-PP (B.E.-II) dated 29th May 2019, revision order no DPIIT Order No. P-45021/2/2017-PP(BE-II) dated June 04, 2020, revision order no. P-45021/2/2017-PP (B.E.-II) dated 16th Sept 2020 and subsequent revision Order No. P-45021/2/2017-PP (BE-ll)-Part(4) Vol. II dated 19/07/2024 & its clarifications/amendment (if any).

Bank will follow the above orders and guidelines on Public Procurement (Preference to Make in India) and basis of allotment will be done in terms of the same.

i. Definitions: For the purpose of this RFP

a. 'Local content' means the amount of value added in India which shall, unless otherwise prescribed by the nodal ministry, be the total value of the item procured (excluding net domestic indirect taxes) minus the value of imported

content in the item (including all customs duties) as a proportion of the total value, in percent.

b. 'Class-I local supplier' means a supplier or service provider, whose goods, services or works offered for procurement, has local content equal to or more than 50%, as defined under this Order.

c. 'Class-II local supplier' means a supplier or service provider, whose goods, services or works offered for procurement, has local content more than 20% but less than 50%, as defined under this Order.

d. 'Non - Local supplier' means a supplier or service provider, whose goods, services or works offered for procurement, has local content less than or equal to 20%, as defined under this Order.

e. 'L1' means the lowest tender or lowest commercial bid or the lowest quotation received in an RFP, bidding process or other procurement solicitation as adjudged in the evaluation process as per the RFP or other procurement solicitation.

f. 'Margin of purchase preference' means the maximum extent to which the price quoted by a "Class-I local supplier' may be above the L1 for the purpose of purchase preference.

ii. Eligibility of 'Class-I local supplier'/ 'Class-II local supplier'/ 'Non-local suppliers' for different types of procurement

a. In procurement of all goods, services or works in respect of which the Nodal Ministry/Department has communicated that there is sufficient local capacity and local competition, only 'Class-I local supplier', as defined under the Order, shall be eligible to bid irrespective of purchase value.

b. In procurement of all goods, services or works, not covered by sub-para ii(a) above, and with estimated value of purchases less than Rs. 200 Crore, in accordance with Rule 161(iv) of GFR, 2017, Global tender enquiry shall not be issued except with the approval of competent authority as designated by Department of Expenditure. Only 'Class-I local supplier' and 'Class-II local supplier', as defined under the Order, shall be eligible to bid in procurements undertaken by procuring entities, except when Global tender enquiry has been issued. In global tender enquiries, 'Non-local suppliers' shall also be eligible to bid along with 'Class-I local suppliers' and 'Class-II local suppliers.

iii. Purchase Preference

a. Subject to the provisions of this Order and to any specific instructions issued by the Nodal Ministry or in pursuance of this Order, purchase preference shall be given to 'Class-I local supplier' in procurements undertaken by bank in the manner specified here under.

b. In the procurements of goods or works which are covered by para ii(b) above and which are divisible in nature, the 'Class-I local supplier shall get

purchase preference over 'Class-II local supplier', as per following procedure:

1. In case there is sufficient local capacity and competition for the item to be procured, as noted by the nodal ministry, only class I local suppliers shall be eligible to bid. As such, the multiple suppliers, who would be awarded the contract, should be all and only 'Class-I local suppliers'

2. In other cases, 'Class II local suppliers may also participate in the bidding process along with 'Class-I local suppliers' as per provisions of this Order.

3. If 'Class-I local suppliers' qualify for award of contract for at least 50% of the tendered quantity, the contract will be awarded to all the qualified bidders as per the award criteria stipulated in the bid document. However, in case 'Class-I local suppliers' do not qualify for award for contract for at least 50% of the tendered quantity, purchase preference will be given to the 'Class-I local suppliers' over 'Class-II local suppliers' provided that their quoted rate falls within 20% margin of purchase preference of the highest quoted considered for award of contract so as to ensure that the 'Class-I local suppliers' taken in totality are considered for award of contract for at least 50% of the tendered quantity.

4. First purchase preference will be given to the lowest quoting 'Class-I local suppliers', whose quoted rates fall within 20% margin of purchase preference, subject to its meeting the prescribed criteria for award of contract as also the constraint of maximum quantity that can be sourced from any single supplier. If the lowest quoting 'Class-I local suppliers', does not qualify for purchase preference because of aforesaid constraints or does not accept the offered quantity, an opportunity may be given to next higher 'Class-I local suppliers', falling within 20% margin of purchase preference, and so on.

5. To avoid any ambiguity during bid evaluation process, Bank may stipulate its own RFP/tender specific criteria for award of contract amongst different bidders including the procedure for purchase preference to 'Class-I local suppliers' within the broad policy guidelines stipulated in sub-paras above.

iv. Margin of Purchase Preference: The margin of purchase preference shall be 20%.

v. Verification of Local Content:

a. The 'Class-I local Supplier'/ 'Class-II local Supplier' at the time of tender, bidding or solicitation shall be required to indicate percentage of local content and provide Self-certification that the item offered meets the local content requirement for 'Class-I local supplier'/ 'Class-II local Supplier', as the case may be. They shall also give details of the location(s) at which the local value addition is made.

b. In case of procurement for a value in excess of Rs. 10 crores, the 'Class-I Local Supplier/'Class-II Local Supplier' shall be required to provide a certificate from the statutory auditor or cost auditor of the company (in the case of companies) or from a practicing cost accountant or practicing chartered accountant (In respect of suppliers other than companies) giving the percentage of local content.

c. False declarations will be in breach of the Code of Integrity under Rule 175(1)(i)(h) of the General Financial Rules for which a bidder or its successors can be debarred for up to two years as per Rule 151 (iii) of the General Financial Rules along with such other actions as may be permissible under law.

d. A supplier who has been debarred by any procuring entity for violation of this Order shall not be eligible for preference under this Order for procurement by any other procuring entity for the duration of the debarment. The debarment for such other procuring entities shall take effect prospectively from the date on which it comes to the notice of other procuring entities.

vi. If nodal ministry is satisfied and communicates to bank that Indian suppliers of an item are not allowed to participate and /or compete in procurement by any foreign government, it may, if it deems appropriate, restrict or exclude bidders from that country from eligibility for procurement of that item as per advise of nodal ministry.

For the Purpose of above, a Supplier or bidder shall be considered to be from a country if (i) the entity is incorporated in that country, or ii) a majority of its shareholding or effective control of the entity is exercised from that country; or (iii) more than 50% of the value of the item being Supplied has been added in that country. Indian suppliers shall mean those entities which meet any of these tests with respect to India." Declaration to be submitted by bidder as per Annexure-IX.

7. Bank will also provide benefits to Micro and Small Enterprises (MSEs) as per the guidelines of public procurement policy issued by Government of India. The bidders to submit declaration for claiming MSE Benefits as per Annexure-VII.

8. **RESTRICTION OF BIDDERS FROM COUNTRIES SHARING LAND BORDERS WITH INDIA:**

As per Ministry of Finance, Department of Expenditure, Public Procurement Division's office memorandum F.No.6/18/2019-PPD dated 23.07.2020, regarding insertion of Rule 144 (xi) in the General Financial Rules (GFR) 2017, any bidder from a country which shares a land border with India will be eligible to bid either as a single entity or as a member of a JV / Consortium with others, in any procurement whether of goods, services (including consultancy services and non-consultancy services) or works (including turnkey projects) only if the bidder is registered with the Competent Authority. The Competent Authority for registration will be the Registration Committee constituted by the Department for Promotion of Industry and Internal Trade (DPIIT). Political & Security

clearance from the Ministries of External and Home Affairs respectively will be mandatory.

However, above condition shall not apply to bidders from those countries (even if sharing a land border with India) to which the Government of India has extended lines of credit or in which the Government of India is engaged in development projects. Updated lists of countries to which lines of credit have been extended or in which development projects are undertaken are given in the website of the Ministry of External Affairs (MEA).

“The successful bidder shall not be allowed to sub-contract works to any contractor from a country which shares a land border with India unless such contractor is registered with the Competent Authority”

Definitions pertaining to “Restriction of Bidders from Countries sharing Land Borders with India” Clause Bidder" (including the term 'tenderer', 'consultant' 'vendor' or 'service provider' in certain contexts) means any person or firm or company, including any member of a consortium or joint venture (that is an association of several persons, or firms or companies), every artificial juridical person not falling in any of the descriptions of bidders stated hereinbefore, including any agency, branch or office controlled by such person, participating in a procurement process.

"Bidder from a country which shares a land border with India" means:

a) An entity incorporated, established or registered in such a country; or

b) A subsidiary of an entity incorporated, established or registered in such a country; or

c) An entity substantially controlled through entities incorporated, established or registered in such a country; or

d) An entity whose beneficial owner is situated in such a country; or

e) An Indian (or other) agent of such an entity; or

f) A natural person who is a citizen of such a country; or

g) A consortium or joint venture where any member of the consortium or joint venture falls under any of the above

"Beneficial owner" will be as under:

i. In case of a company or Limited Liability Partnership (LLP), the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person(s), has a controlling ownership interest or who exercises control through other means.

Explanation

a. "Controlling ownership interest" means ownership of, or entitlement to, more than twenty-five per cent of shares or capital or profits of the company;

b. "Control" shall include the right to appoint the majority of the directors or to control the management or policy decisions, including by virtue of their shareholding or management rights or share-holders' agreements or voting agreements;

ii. In case of a partnership firm, the beneficial owner is the natural person(s) who, whether acting alone or together, or through one or more juridical person, has ownership of entitlement to more than fifteen percent of capital or profits of the partnership;

iii. In case of an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of or entitlement to more than fifteen percent of the property or capital or profits of such association or body of individuals;

iv. Where no natural person is identified under (i) or (ii) or (iii) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

v. In case of a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with fifteen percent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

"Agent" is a person employed to do any act for another, or to represent another in dealings with third persons.

9. Please note that

(i) The cost of preparing the bids, including visit / visits to the Bank is not reimbursable.

(ii) Each Recipient should notify the Bank of any error, fault, omission, or discrepancy found in this RFP document but not later than last date of receiving clarifications.

(iii) The Bank is not bound to accept any of the bids submitted and the bank has the right to reject any/all bid/s or cancel the tender at any point without assigning any reason therefor.

(iv) All pages of the Bid document, Clarifications/Amendments, if any, should be signed by the Authorized Signatory under the seal of the bidder company/ firm and to be uploaded with technical bid. A certificate to the effect that the Authorized Signatory has authority to bind the company/ firm should also be attached along with the technical bid.

(v) The Authority/Bank shall not be liable for any omission, mistake or error in respect of any of the above or on account of any matter or thing arising out of or concerning or relating to RFP, Bidding Documents or the Bidding Process, including any error or mistake therein or in any information or data given by the Authority.

(vi) Nothing in this RFP shall obligate either Party to enter into any further Agreements.

After technical evaluation, intimation will be given to all qualifying bidders about the date and time of reverse auction through email alert from GeM.

Note: The tender cannot be split. Either the Bidder on behalf of the Principal/ OEM or the Principal/ OEM themselves can participate in the bid, but both cannot bid simultaneously for the same solution. Consortium is not allowed in this RFP.

SECTION-II

INSTRUCTIONS TO BIDDERS

1. Introduction

The Bidder is expected to examine all instructions, forms, terms and specifications given in the Bidding Documents. If any element of doubt arises, the same should be clarified from the Bank in terms of this RFP. Failure to furnish all information required in the Bidding Documents may result in the rejection of its bid and will be at the Bidder's own risk. Bank shall not be responsible for the same.

2. Pre-Bid Meeting

a. A pre-bid meeting is scheduled to be held through physical/Video Conference/ Web-ex on 26.09.2025 3:00 PM. Bidder's designated representatives (maximum two persons) may attend the pre-bid meeting.

b. The purpose of the meeting will be to clarify the doubts raised by the probable bidders.

c. The Bidder is requested to submit any queries/clarifications to the Bank to the following email ids on or before 25.09.2025 05:00 PM.

Email id:
arvind.kumar@indianbank.co.in
anil.lakra@indianbank.co.in
sreehari.t@indianbank.co.in
Rikesh.Shah@indianbank.co.in

In case the Probable Bidder wants to participate in the Pre-Bid Meeting to be held on the date specified in this bid, they should send their request for the same on the above-mentioned email-ids. On receiving Bidders' e-mail request for Pre-Bid Meeting, the meeting details will be e-mailed to Bidder. But bidder may join the meeting online.

Venue for Pre-Bid meeting:

Indian Bank, Head Office,
66 Rajaji Salai,
Ground Floor,
Information System Security Department,
Chennai – 600001

The text of the questions raised and the responses given, together with amendment to the bid document, if any, will be posted in websites: https://www.indianbank.bank.in and GeM portal (without identifying the source of enquiry).

3. Amendment of bidding documents

3.1 At any time prior to the deadline for submission of bids, the Bank, for any reason, whether at its own initiative or in response to a clarification(s) requested by a prospective Bidder, may modify/ cancel/ extend/ amend the Bidding Document by modification(s) / amendment(s).

3.2 The amendments & clarifications if any, will be published in Bank website and in the GeM Portal and will form part of the Bidding document.

3.3 Any bid submitted by a bidder under this RFP process cannot be withdrawn / modified after the last date for submission of the bids unless specifically permitted in writing by the Bank.

3.4 No bid shall be withdrawn in the intervening period between deadline for submission of bids and expiration of period of bid validity. In the event of withdrawal of the bid by bidders, default bidder will be suspended from participating in future tenders of bank. The bank may extend the period of bid validity before its expiration, in case Bank desires.

3.5 No bidder shall be allowed to withdraw the bid if bidder happens to be successful bidder.

4. Technical Bid

The Bidder shall furnish as part of its technical bid, documents establishing the bidder's eligibility to bid and its qualifications to perform the Contract.

The documentary evidence of the Bidder's eligibility to bid and qualifications to perform the Contract if its bid is accepted, shall establish to the Bank's satisfaction that, the Bidder has the financial and technical capability necessary to perform the Contract and that, the Bidder meets the qualification requirements.

Any bid document not accompanied by the above will be rejected.

5. Commercial Bid

At the time of submission of technical bid, Bidder has to submit the commercial bid. The commercial bids submitted by the bidder will be considered as the sealed online bid for the RFP. The commercial bids of technically qualified bidders will be opened by Bank and reverse auction will be conducted for the RFP. The GeM may eliminate the H1 bidders from the reverse auction process as per the elimination rule defined in the GeM bid document and intimation will be sent by GeM to those bidders who are eligible for the reverse auction, after H1 elimination. The final price quoted by bidders during reverse auction (RA) process will be taken as the commercial offer of that bidder. In case bidder/s doesn't quote any price in the reverse auction, then Bank will consider the online commercial bid submitted by bidder/s at the time of technical bid as their final commercial offer (as per GeM terms) and bid will be evaluated accordingly.

6. Clarification of Bids

During evaluation of the bids, the Bank may, at its discretion, seek clarification from the Bidder/s. The request for clarification and the response shall be submitted in GeM, and no change in the substance of the bid shall be sought, offered, or permitted.

The Bidder shall make his/her own interpretation of any and all information provided in the Bidding Document. The Bank shall not be responsible for the accuracy or completeness of such information and/or interpretation. Although certain information are provided in the Bidding Document, however, bidder shall be responsible for obtaining and verifying all

necessary data and information, as required by him. The Bank shall not be bound to accept the lowest tender and reserves the right to accept any or more tenders in part. Decision of Bank in this regard shall be final.

7. Bid Security (Earnest Money Deposit)

The Bidder should submit at the time of online submission of Bid, as part of its bid, a bid security / EMD in the form of DD/ Fund transfer/ Bank Guarantee issued by a Scheduled Commercial Bank located in India (other than Indian Bank), in the form provided in the Bidding Documents (Annexure-XIV) for a sum of Rs.15,00,000/- valid for 225 days from the last date for submission of Bid. Bank may seek extension of Bank Guarantee, if required. Relaxation if any, extended by GOI/ competent authorities for furnishing the EMD shall be passed on to the bidders.

Unsuccessful Bidders' Bid Security will be discharged or returned once the procurement process is completed. The successful Bidder's Bid Security will be discharged upon the Bidder signing the Contract and furnishing the performance security.

The bid security may be forfeited if:

a) Bidder withdraws its bid during the period of bid validity or does not accept the correction of errors in accordance with the terms of RFP;

or

b) In the case of a successful Bidder, if the Bidder fails or refuses to sign the Contract within the specified time from the date of issue of purchase order or fails or refuses to furnish performance security.

Please note: Relaxation if any, extended by GOI/ competent authorities for furnishing EMD shall be passed on to eligible bidders.

MSE/NSIC registered bidders are exempted from submitting the bid security. Such bidders should submit the copy of registration certificate and other document along with declaration as per section Annexure-VII for claiming exemption for bid security, as proof which should be valid for the current period.

If the bidder wants to avail the Purchase preference, the bidder must be the manufacturer of the offered product in case of bid for supply of goods. Traders are excluded from the purview of Public Procurement Policy for Micro and Small Enterprises.

8. Evaluation Criteria

Bid evaluation methodology that Indian Bank is adopting is given below:

Opening of bids:

- Opening of Eligibility cum Technical bid

a) The Eligibility cum Technical bid shall be opened by Bank as per the schedule mentioned in the RFP document and its subsequent amendment.

b) Bank however reserves the right to change the date & time for opening of Eligibility cum Technical bid without assigning any reason whatsoever. In case there is a

change in the schedule the same will be intimated to the bidders by putting up on the Bank's website.

c) Bidders who qualify the eligibility criteria, technical specifications will be called as technically qualified bidder.

➢ Opening of Commercial bid

After eligibility cum technical bid evaluation is completed, Bank will open commercial bids of eligible and technically qualified bidders only, as per GeM terms. Subsequently, Bank will conduct the reverse auction among the technically qualified bidders as per the terms & conditions mentioned in RFP document.

➢ Evaluation of Bids

The evaluation/ selection process will be done with combination of eligibility, technical competence and commercial aspects.

➢ Eligibility Evaluation

Eligibility evaluation will be done to ascertain the eligibility of the vendor/ service provider/ system integrator to bid for the project. Only those bidders who fulfil the minimum eligibility criteria mentioned under next heading will proceed to the next step.

8.1 Eligibility Criteria

Bank is looking for eligible bidders for selecting a vendor for Incident Response (IR), Cyber/Digital forensic services, Red Team, Tabletop & Cyber Drill Exercise. Only those Bidders who fulfil the following criteria are eligible to respond to the RFP. Offers received from Bidders who do not fulfil any of the following eligibility criteria are liable for rejection.

The bidder must fulfil the criteria mentioned in the table below in order to bid for this RFP:

S. No.	Eligibility Criteria	Supporting Documents to be Submitted	Compliance (Y/N)
1	The bidder should be registered as a company in India as per Companies Act 1956 OR Companies Act 2013 OR Partnership Bidder registered under LLP Act, 2008, operating since last 5 years as on the date of Bid Submission date of RFP.	Certificate of Incorporation or any other certificate of registration issued by competent authority from Government of India. In case of mergers/ acquisitions/ restructuring/ splitting/ de-merger or name change (of the Bidding Entity), the date of establishment of earlier/ original partnership firm/ limited company shall be taken into account. Copy of Certificate of Incorporation issued by the ROC and Articles of Association should be submitted. All Documents related to the mergers/ acquisitions/ restructuring/ splitting/ de-merger or name change (of the Bidding Entity) like board resolution, NCLT Resolution etc. should be submitted.	

2	The bidder should have minimum average annual turnover of Rs. 15 Crores (Rupees Fifteen Crores only) (Rs.10 Cr – Rupees Ten Crores only for MSE/Startups Bidders) from Indian operations in each of the latest three out of four financial years i.e., 2021-22, 2022-23,2023-2024 and 2024-25. This must be the individual company turnover from India Operations and not that of any group of companies.	Copy of Auditor certificate for the financial years 2022-23, 2023-24 and 2024-25). Note: The CA certificate provided in this regard should be without any riders or qualification. Copies of latest three out of four years' audited balance sheet. For MSE relaxation in terms of prior turnover, 1. Claim EMD exemption. 2. Credentials should be verifiable online through Udyam Registration website of Ministry of MSME as per the supporting documents uploaded during bidding process	
3	The bidder must have successfully provided IRR/Cyber security retainer/Cyber incidence response services in at least One PSU/ Government/ BFSI / listed private organizations in India, during last Five years.	Bidder has to submit the following documents: (i) Copy of Purchase Order/ Work Order/ Agreement signed & stamped by the Client. **AND** (ii) Copy of Performance Certificate as per Annexure - IV in hardcopy/softcopy/email **OR** Performance certificate/ Mail confirmation from client clearly stating the product name, model/version deployed, that the same is successfully running as on date, The date/month of commissioning/go-live and that the performance of the Bidder as well as the product deployed is satisfactory.	
4	The bidder must have at least any ONE of the below mentioned Certifications such as SOC 1, SOC 2, SOC 3, ISO 27001-2022, ISO 27005, ISO 22301, NIST, CSA-STAR, GDPR, EU-U.S. and Swiss-U.S.	Bidder must submit at least any two of mentioned certifications.	

	Privacy Shield Frameworks or Indian equivalent certifications acceptable as per Bank's discretion. The bidder must be Cert-in empanelled.		
5	The bidder must have at least 10 relevant skillsets resources on its payroll possessing at least any two of the following professional certifications or their Indian equivalent certifications as per Bank's discretion: • GIAC Cyber Threat Intelligence (GCTI), or • GIAC Certified Forensic Analyst (GCFA), or • GIAC Certified Incident Handler Certification (GCIH) or • EC-Council Certified Incident Handler v2 (E|CIH), or • Certified Information Systems Security Professional (CISSP) or • GIAC Cloud Forensics Responder (GCFR) or • GIAC Network Forensic Analyst (GNFA) or • GIAC Reverse Engineering Malware	The Bidder must submit the details of the resources on its letterhead along with the relevant certificate.	

	Certification (GREM) or • Computer Hacking Forensic Investigator (CHFI) or • Offensive Security Certified Professional (OSCP) • Certified Ethical Hacker (CEH)		
6	The bidder should not be involved in any litigation which threatens solvency of company.	Certificate is to be provided by the chartered accountant /statutory auditor	
7	The Bidder should not have been blacklisted/ debarred /banned by Government/Government agency / Banks / Financial Institutions / PSUs in India during last 3 years as on bid submission date.	Certificate is to be provided as per Annexure - II	
8	The Bidder to provide information that none of its subsidiary or associate or holding company or companies having common director/s or companies in the same group of promoters/management or partnership firms/LLPs having common partners is not owned by any Director or Employee of the Bank.	Self-undertaking to be submitted on company letter head.	
9	Labour Law Compliances	Undertaking on Bidders letterhead as per Annexure - X.	
10	The net worth of the Bidder firm should not be negative as on 31.03.2025 and also	Copy of audited financial statements/certificate from CA with Net worth details of three financial years need to be submitted. In case	

	should not have eroded by more than 30% (thirty percent) in the last 3 preceding Financial Years (FY 2022-23, FY 2023-24 & FY 2024-25).	audited balance sheet is not available for 2024-25, the company may provide provisional balance sheet duly signed by Charted Accountant.	

Note:

a. Bidder must comply with all above-mentioned criteria. Non-compliance of any of the criteria will entail rejection of the offer summarily.
b. Photocopies of relevant documents/ certificates should be submitted as proof in support of the claims made. Indian Bank reserves the right to verify/ evaluate the claims made by the bidder, independently or by virtue of a third party. Any decision of Indian Bank in this regard shall be final, conclusive and binding upon the bidders.

Once the bidders qualify the eligibility criteria, they will be eligible for the Technical Bid Evaluation. Offers received from the bidders who do not fulfil all or any of the above eligibility criteria are liable to be rejected.

General Evaluation Criteria

i. The Bank will examine the bids to determine whether they are complete, whether any computational errors have been made, whether required sureties have been furnished, whether the documents have been properly signed, and whether the bids are generally in order.
ii. The Bank may waive any minor informality, non-conformity, or irregularity in a bid which does not constitute a material deviation, provided such waiver does not prejudice or affect the eligibility of any Bidder.
iii. Prior to the detailed evaluation, the Bank will determine the substantial responsiveness of each bid to the bidding documents. For purposes of these clauses, a substantially responsive bid is one which conforms to all the terms and conditions of the Bidding Documents without material deviations.

8.2 Technical Evaluation

The Bidder should satisfy all the Eligibility Criteria mentioned in RFP and the hardware/software offered by them should meet all the Technical Specifications stipulated in the bid. Further Bidder should also submit all the required annexures/proofs asked in the RFP document.

The Bidder who complies all the above criteria will be declared technically qualified bidder.

8.3 Commercial Evaluation

The bidder should quote the cost (inclusive of all taxes) as mentioned in the commercial bid format (Part-II of RFP) while submitting the bid in GeM portal.

COMMERCIAL BID of only those bidders will be opened in GeM portal, who will comply with all the eligibility criteria, will confirm compliance to all the terms & conditions of RFP document, in the Technical Evaluation Stage. After opening of the commercial bids of the technically qualified bidders, Bank will conduct the reverse auction among the bidders to

arrive at final commercial offer of the bidders. However, Highest Quoted Commercial (H1) Bidder will be eliminated from the reverse auction process, if more than three bidders are found technically qualified. Bidder shall quote all the figures in numbers followed by total in words enclosed in brackets in all fields of commercial bid.

In the Reverse Auction, the bidder will be required to quote commercial as per Commercial Bid Format. The price quoted should be inclusive of all charges and taxes. The bidder who quotes lowest amount will be identified as successful bidder. The successful bidder has to submit price break-up as per commercial bid format within five (5) working days, post completion of Reverse Auction process directly to Bank duly signed by the authorised signatory. The unit price for each line item should be comparable to prevailing market rates.

Note: Working days here refers to Bank's working days in Chennai, Tamil Nadu.

8.4 Commercial Evaluation Methodology

1. The Bank will evaluate the commercial bids on the basis of the **Total Cost of Ownership (TCO) for a period of 3 years**.

2. Bidders are required to quote rates strictly as per the **Commercial Bid Format (Part II – Commercial Bid)**. Any deviation or conditional pricing will lead to rejection of the bid.

3. To ensure uniformity and fairness, the Bank will apply the following Frequency for evaluation purposes. Actual payments will be made on the basis of actual usage, but the below assumptions will be used only for commercial comparison:

Sl. No.	Service Component	Frequency (for 3 years)
1	Incident Response Readiness Assessment	3 (One every year)
2	Cyber/Digital Forensic Readiness Assessment	3 (One every year)
3	On-demand Incident Response Support	15 man-days**
4	On-demand Cyber/Digital Forensic Audit/Investigation/Analysis	15 man-days**
5	Red Team	3 (One every year)
6	Cyber Drill	3 (One every year)
7	Tabletop Exercise	3 (One every year)

** man-days = working of one person for one day. It will be used for arriving the L1 vendor and finalizing the commercial only.

4. The **TCO calculation** will be as follows:

    - TCO = (Cost of Annual Readiness Assessments for 3 years) + (Cost of Cyber/Digital Forensic Readiness Assessments for 3 years) + (Cost of assumed On-demand Incident Response support or 15 man-days) + (Cost of assumed Forensic engagements or 15 man-days) + (Cost of 9 Exercises - Red Team / Cyber Drill / Tabletop each per year).

5. The bidder with the **lowest TCO (L1)** will be considered for selection, subject to meeting all technical and eligibility requirements.
6. All prices shall be quoted in INR, inclusive of applicable taxes.
7. The quoted rates shall remain firm and unchanged for the entire contract period of 3 years.

8.5 Correction of Error in Commercial Bid

Bank reserves the right to correct any arithmetical errors furnished in the Commercial Bid. If any such errors are noticed, it will be rectified on the following basis:

(a) Bank may waive off any minor infirmity or non-conformity or irregularity in a bid, which does not constitute a material deviation.

(b) Price quoted by Bidder in figures in GeM portal will be considered for commercial evaluation.

If the bidder does not accept the correction of errors, the bid will be rejected and EMD may be forfeited.

9. Proposal Process Management

The Bank reserves the right to accept or reject any or all proposals received in response to the RFP without assigning any reasons thereof. Also, the Bank reserves rights to revise the RFP, to request one or more re-submissions or clarifications from one or more Bidders, or to cancel the process in part or whole without assigning any reasons. Additionally, Bank reserves the right to alter the requirements, in part or whole, during the RFP process, and without re-issuing the RFP.

Each party shall be entirely responsible for its own costs and expenses that are incurred in the RFP process, including presentations, demos and any other meetings.

10. Liabilities of the Bank

This RFP is not an offer by Bank, but an invitation for bidder responses. No contractual obligation on behalf of Bank whatsoever shall arise from the RFP process unless and until a formal contract is signed and executed by duly authorized officials of Bank and the bidder.

11. Bid and Proposal Ownership

The Bid submitted and all supporting documentation/ templates are the sole property of Indian Bank and should NOT be redistributed, either in full or in part thereof, without the prior written consent of Bank. Violation of this would be a breach of trust and may, inter-alia causes the Bidder to be irrevocably disqualified. The proposal and all supporting documentation submitted by the Bidder shall become the property of Indian Bank and will not be returned. Recipients shall be deemed to license, and grant all rights to Bank, to reproduce the whole or any portion of their submission for the purpose of evaluation and to disclose and/or use the contents of the submission as the basis for any resulting RFP

process, notwithstanding any copyright or other intellectual property right that may subsist in the submission or Banking documents.

If related parties (as defined below) submit more than one Bid, then both/ all bids submitted by related parties are liable to be rejected at any stage at Bank's discretion:

a) Bids submitted by holding company and its subsidiary company.
b) Bids submitted by two or more companies having common director/s
c) Bids submitted by companies in the same group of promoters/management etc.
d) Either the Bidder on behalf of the Principal/ OEM or the Principal/ OEM themselves can participate in the bid, but both cannot bid simultaneously for the same solution.

12. Bid Pricing Information

By submitting a signed bid, the Bidder certifies that:

(a) The Bidder has arrived at the prices in its bid without agreement with any other bidder of this RFP for the purpose of restricting competition; and
(b) The prices in the bid have not been disclosed and will not be disclosed to any other bidder of this RFP; and
(c) No attempt, to induce any other bidder to submit or not to submit a bid for restricting competition, has occurred.

GeM Bid Ref: GEM/2025/B/6707442 **Date:** ***20.09.2025***

SECTION – III

Broad Scope of Work

CONDITIONS OF CONTRACT

1) Scope of work

The Bank invites proposals from eligible and experienced service providers for the engagement of the following cybersecurity services, to be delivered on an annual and on demand basis:

1. **Incident Response Readiness Assessment (Annual)** – Evaluation of the Bank's preparedness to detect, respond to, and recover from cyber incidents.
2. **Incident Response Support (On-Demand)** – Expert assistance during the security breach, immediate detection, containment, and remediation to minimize damage and quickly restore normal operations.
3. **Cyber/Digital Forensics Readiness Assessment (Annual)** – Assessment of the Bank's forensic capabilities, tools, and procedures to ensure effective investigation and evidence handling.
4. **Cyber/Digital Forensics Incident Audit / Investigation / Analysis (On-Demand)** – Expert-led forensic analysis and investigation of cyber incidents as and when required.
5. **Red Team Exercises (Annual)** – Simulated adversarial attacks to evaluate the Bank's detection and response capabilities.
6. **Cyber Drills (Annual)** – Scenario-based technical drills to test incident response mechanisms. These may be conducted biannually at the discretion of the Bank.
7. **Tabletop Exercises (Annual)** – Simulated, discussion-based exercises to assess decision-making and coordination during cyber incidents.

Service providers must demonstrate relevant domain expertise, industry certifications, and a proven track record in delivering similar engagements to financial institutions. All services shall be delivered in accordance with applicable regulatory guidelines and industry best practices.

Broad Scope of work for Incident Response:

Phase 1:

1. **Incident Response Readiness Assessment (IRRA)**

   This phase will include review of existing monitoring, logging and detection technologies, current network and host architecture, evaluating first response capabilities and Improve Bank's Incident Response Plan and Procedures. Vendor will help the Bank to establish an incident response capability so that Bank is ready to respond to it. Under this preparation phase, which involves preparing for potential cyber incidents by establishing incident response plans, identifying the procedural and technical gaps in existing IT Setup w.r.t. incident response readiness, creating an incident response team having representative from Bank and IR vendor personals, defining their roles and responsibilities, and implementing monitoring and detection systems.

   Workshops/assessment to be conducted with various stakeholders in the Bank by bidder in order to understand Bank environment to enable to Bidders Incident response

team to respond, mitigate, recover from attacks as soon as possible. This phase is to review banks existing Incident response plans, technologies deployed, log sources in place to detect/analyses to be checked and reediness in order to respond to attacks/breaches within stipulated timelines. The vendor should perform the gap assessment on existing SOP of Cyber Security incident handling/ Cyber crisis management plan and various other procedure documents.

2. The IRRA should not be only limited to meetings/workshops/trainings, but Infrastructure manipulation capabilities also to be assessed based on various real time use cases, but not limited to:
    I. Centralized deployment/execution of IOC scanners or other tools designed to obtain digital evidence.
    II. Credentials management (e.g. password change policies)
    III. System backup architecture and backup recovery.
    IV. Logging security event sources
    V. Log sources / security controls check.
    VI. Assessment of readiness to respond, mitigate, recover from various attack scenarios, but not limited to;
        a. Espionage by threat actors (including state-sponsored groups)
        b. Watering hole attacks
        c. Trusted relationship attacks
        d. Supply chain attacks
        e. Money theft through online banking systems, card processing etc.
        f. ATM jackpotting
        g. Ransomware attacks
        h. Unauthorized access to servers, databases, web applications, network equipment etc.
        i. Insider attacks (leaks, disruption, sabotage, unauthorized access etc.)
        j. Infection using botnets.
        k. Phishing campaigns (links & attachments)
        l. Cryptocurrency mining malware attacks
    VII. The log sources / security controls should include, but not limited to
        a. DHCP logs
        b. DNS logs
        c. Network traffic logs
        d. Event logs from endpoints and servers (at the OS level), network & security devices like DLP, EDR, WAF, Firewall, HIPS, VPN, Active Directory etc.
        e. Logs of user authorization and activities on business systems
        f. Audit logs of user actions on virtual machine servers & cloud platforms.
3. The vendor will help the Bank to prepare incident response team's specific technical methods, strategies, checklists, and forms based on gap assessment.
4. The vendor will provide recommendations on how to improve incident response readiness.
5. The vendor will provide recommendations on how to reconfigure or upgrade existing security event monitoring.
6. The vendor will setup the dedicated IT infrastructure for Indian Bank within India, either physical or in cloud instance (cloud region should be located within India or specific the region of the Incident occurrence), which will be utilized and accessed remotely by IR analysts, during incident response for log analysis and correlation. No logs or metadata should be transferred outside of India. The cloud instances should be preserved at

least for 3 years at the end of contract or based on agreed retention period as per Bank written confirmation.

7. During Incident response readiness review exercise the vendor should clearly define below modalities in detail.
   - Incident Response team structure and responsibilities
   - Communication between different teams (IR, ISSD and other stakeholders from Bank) will take place in case of Cyber Incident
   - Procedure of sharing evidence / access to the required logs.
   - The selected vendor will help Bank to prepare and regularly update for the Bank.
8. Establishing required Infrastructure to handle Cyber Incident/ sharing evidence:
   - The successful vendor should establish a process, and deploy/install necessary hardware, software, sensors, scripts, agents for collection of evidence for incident analysis.
   - Assist in clearing/signoff of security review of such tools, devices, and technologies before completion of Phase 1 (IRRA) from bank's side.
9. Recommendations on how to reconfigure or upgrade existing security event monitoring systems, backup solutions, security devices, etc.
10. Provide Incident Response Readiness Assessment Guide.
11. Provide Incident Response Readiness Assessment Report.

Phase 2: Incident Identification

The required manpower and number of days will be utilized in onwards phases, on actual utilization and deployment of IR services.

1. This phase will involve identifying and categorization (e.g., critical, high, medium, low priority) of potential incident in co-ordination with Bank by collecting and analyzing data from various sources, such as intrusion detection systems, log files, applications, devices and network traffic etc.
2. 24*7*365 days dedicated support facility for incident response shall made available by the vendor. The vendor IR staff should be well trained to effectively handle queries raised by the Bank, whenever a phone call/ email /alert received from Bank's dedicated Officials for probable incident.
3. The Service provider should acknowledge receipt of alert from bank within 2 Hours and start the Incident Response within 4 Hours of reporting of alert from the Bank. Upon confirmed breach, the IR analyst should immediately start working on preliminary information submitted by the Bank. At least 2 IR analyst should be at onsite location (DC, DR, NDR, NDC, HO or CO) of breach, if required, within 24 Hours, excluding travel time.
4. Provide detailed information of the Threat Adversary identified in the initial assessment based on intelligence of service provider and experience.
5. An IR daily status update that covers the days' status summary, action items, intelligence summary, and current recommendations to be provided to bank in writing.
6. Service provider to ensure incident response and forensic investigation report has to be duly vetted by CERT-In empanelled auditor, which should be acceptable to regulators of India.
7. A walkthrough meeting to be conducted on reported findings.

Phase 3: Containment

In this phase, the IR (incident response) team will work to contain the incident to prevent the further damage to affected IT assets and ensure that other IT systems remain unaffected. The bidder shall assist in reporting and notification to Regulatory and statutory authorities, Law Enforcement Agencies, Bank's Public Relations &. Social Media Department, Human Resource Department, News publication etc.

Phase 4: Analysis

This phase will involve analyzing the incident to determine the scope, cause, and extent of the damage. The IR team may further gather and examine evidence, interview witnesses, and use forensic tools to identify the attacker and their methods.

1. Log retention and the logs collected/processed should be available for export in supported formats and not associated without any proprietary formats for audit/compliance purposes.
2. The vendor should be able to perform investigation on different technologies, assets inclusive of all technologies, applications, devices available in Bank's IT-Ecosystem and the various resources required during the investigation should be scalable.

Phase 5: Eradication

The vendor should identify and mitigating all vulnerabilities that were exploited by the Threat Actor. This phase involves removing the threat from affected systems completely to bring to their original state.

Phase 6: Recovery/Monitoring:

In this phase, the incident response team works to restore the attacked system/ operations to normal state and should ensure that the systems are functioning normally and remediate vulnerabilities to prevent similar incidents in the bank. The bidder should perform continuous monitoring of the network/in for the agreed period of time based on the severity of incident in order to make sure that there is no remanence of the threat actor left in the network.

Phase 7: Reporting & Lesson learned:

The successful vendor should provide User awareness training, updating relevant policies and procedures, and reviewing incident response plans and shall also provide;

1. Threat Briefing to Executive Board Members. Assist in reporting and notification to Regulatory and statutory authorities, Law Enforcement Agencies, Bank's Public Relations &. Social Media Department, Human Resource Department, News publication etc.
2. Root cause analysis of the incident for corrective actions to be submitted to Bank for improvements in robustness and resilience in Cyber Security posture of Bank's IT infrastructure.
3. The incident response team should conduct a post incident review to identify what worked well and what could be improved for future incidents and lesson learned. The IR team must give inputs to update Bank's incident response plan and suggest action plan for implementing necessary changes and improvement needed.

Other services to be provided by the Bidder but not limited to:

1. Service provider shall provide the security incident first responder training to key staff members identified by bank to identifying and protecting the scene, preserving evidence, collect data, maintain chain of custody etc.
2. Service provider shall conduct trainings of Bank personnel to ensure proper documentation, procedure, policies during a forensic investigation.
3. Service provider shall understand the legal requirements and implications of forensic investigations including privacy laws and regulations.
4. Service provider shall provide legal evidence which are valid in courts and present the same to the court.
5. Service provider shall develop a forensic response plan mentioning the steps to be taken while collecting & preserving digital evidence after a ransomware attack.
6. Service provider shall determine how critical data is stored and how it can be accessed during forensic investigation.
7. Service provider shall assist regulatory bodies during their forensics investigation, if required.
8. The Incident Response Team/vendor shall be able to use below methodologies for handling of Cyber Incident and response.

1	The Bidder must be able to Conduct host-based sweeping activities.
2	The Bidder must be able to search for malware and tools linked to specific attack groups that are collectively known as Advanced Persistent Threat (APT) groups.
3	The Bidder must be able to utilize a mix of automated and manual techniques to identify indicators of compromise.
4	The Bidder must be able to search for various artifacts not limited to: staging paths, persistence mechanisms, lateral movement mechanisms, registry keys, etc.
5	The Bidder must have to capability to sweep the Endpoint with IOC's related to Custom Malware looking for Persistence Mechanism and Lateral Movement techniques.
6	The Bidder must be able to scan windows end points, servers and virtual environments as a part of the compromise assessment to identify evidence of compromise.
7	The Bidder must have an ability to scan different flavors of Windows, Linux & Unix environments for evidence of compromise.
8	The Bidder must be able to also search for malware and tools associated with on-APT groups.
9	The Bidder must inspect IT systems for IOCs Identifying file names and hashes of known malware and utilities.
10	The Bidder must inspect IT systems for IOCs, Analyzing file import tables of each executable file for specific IOCs
11	The Bidder must inspect IT systems for IOCs Reviewing all running processes and network connections for references to known “hostile” domains.

12	The Bidder must inspect IT systems for IOCs Inspecting registry keys and values associated with known malware, and for persistence mechanisms that could lead to the detection of unknown malware.
13	The Bidder must inspect IT systems for IOCs Identifying specific global mutexes used by processes.
14	The Bidder must inspect IT systems for IOCs Detecting rootkits, hidden files, and hidden processes.
15	The Bidder must be able to analyses Web Shells for evidence collection.
16	The Bidder must be able to analyse event logs generated from different IT systems for evidence collection.
17	The Bidder must be able to automate collection and analysis of evidence and minimize manual activities
18	The Bidder must be able to analyse a majority of assets (at least 85% or higher) and not limit to dipstick analysis on a limited set of assets
19	The Bidder must be able to Conduct network monitoring activities
20	The Bidder must have the capability to sweep the Network with IOC's related to Custom Malware looking for Lateral Movement techniques
21	The Bidder must be able to monitor the Network traffic for Backdoor command and control protocols
22	The Bidder must be able to monitor the Network traffic for Communication to IP addresses that are associated with targeted attacker activity.
23	The Bidder must be able to monitor the Network traffic for Resolution of domain names that associates with targeted attacker activity
24	The Bidder must be able to monitor the Network traffic for Certificates that are used by attackers to encrypt malicious traffic.
25	The Bidder must be able to Conduct log data analysis activities.
26	If required, the bidder must have the ability to perform malware analysis and reverse engineering of malware samples using both automated and manual techniques and provide host-based and network-based indicators that are used to find the malware variants in the wild.
27	If required the Bidder should be able to assist for an incident response, from the initial detection to the final resolution of the incident.
28	The bidder must able to provide Signatures, YARA rules, detection rules, block rules for the solution deployed in Bank environment such AV, SIEM, EDR, IDS/IPS, NBAD, AD, etc. in order to detect the presence of IOC or revert the back the changes made by the attacker.
29	Bidder must be able to perform non- intrusive IR activities such as log collection, scanning activity, IOC scans using inbuilt tools in cases if agent installation or vendor proposed tool installation is not possible.

Broad Scope of work for Cyber / Digital Forensics:
The primary scope is to provide Digital / Cyber Forensic and Incident Investigation services to Indian bank. These services may encompass (but not limited to) Evidence collection, acquisition of data, imaging, examination, recovery and presentation of digital evidence for legal admissibility as determined by Indian bank on need basis.

A) Scope for Cyber / Digital Forensic Readiness Assessment:

As a part of the assessment of the Cyber/Digital Forensic Readiness of the Bank, the vendor after review of the existing Infrastructure of the Bank has to provide an assurance / confirmation to the bank that functioning of the Bank's IT system is in Compliance with –

- Bank's Cyber Crisis Management Plan
- RBI Information Security guidelines, Cert-In guidelines, any other legal requirements.

The vendor should benchmark the Bank's Cyber Crisis Management Plan and IT Data Backup Policy with industrial standard and Government regulations and report the identified gaps / non-compliance.

Initially on the first year of appointment, the Vendor shall conduct Digital/Cyber Forensic Readiness Assessment of Bank's IT Infrastructure in order to analyse, identify and mitigate the deficiencies, if any, in the Forensic Incident handling, Evidence collection and storage capabilities, with provision for yearly review of the findings for the next two years. Yearly review of the Bank's critical IT infrastructure, including revalidation of gaps identified to be done and in case of any changes in the Bank's Digital IT Infrastructure/Environment within the period of engagement (3 years) subsequent to the conduct of initial/previous year assessment after engagement, as intimated by the bank, the Vendor shall be required to reassess the Digital/Cyber Forensic readiness for those Business functions/Applications/Devices and submit report at no extra cost to the Bank. Gaps identified during the yearly assessment has to be closed after revalidations within 3 months of submission of final report of that year.

Deliverables shall include but not limited to provide detailed report at the time of assessment of forensic readiness covering the following aspects:

- Review of network architecture and extant critical business applications
- Review of sufficiency of existing log collection, log retention/Backup/archival processes, Policies /Procedures etc. for network & security devices such as Firewall, Routers, Switches, SIEM etc. and Bank's business applications.
- The vendor shall evaluate various areas of security in a multi layered approach (Web, App, DB layers, network security etc.) covering incidents related to CBS, RTGS, DLP, HR Connect, SWIFT, all alternate delivery channel products (Internet Banking, Payment Banking, Mobile Banking, ATM etc.) and any other product / applications being used by the Bank.
- Review the existing Cyber Incident Handling capabilities in terms of People, Process and Technology

- Identify available sources and sufficiency of different types of potential digital evidence for the identified devices and business applications.
- Identify the additional sources of logs that need to be captured to ensure completeness for conducting incident investigation and this includes the formats of logs and whether they contain meaningful information for investigative purposes and admissible in the court of law.
- Evaluate the procedures followed by IT teams to make the necessary evidence available for investigation.
- Evaluate whether the captured logs are in totality on a sample basis and also validate the basis for selection of samples.
- Identify and validate the procedures carried out by IT team to securely gather legally admissible evidence to meet the Legal, Regulatory requirements such as Cert-In, RBI, NCIIPC etc.
- Collate the information obtained through deep dive analysis and submit a gap analysis report.
- Remediation advisory guidance
- Provide onsite training /awareness to Bank's designated personnel (Minimum 10) in the area of Digital/Cyber Forensic Investigation & related topics in the first year.

The outcome of the overall assessment should enable the bank in:

- Ensuring the overall integrity and continued existence of an organization's computer system and network infrastructure.
- Helping the organization by preparing detailed forensic reports for internal use and legal proceedings. Provide expert testimony in court/regulatory hearings.
- Tracking complicated cases like cyber-attacks, such as Data Theft, Data Leakage, Insider Fraud, Malware attacks, APTs, Ransomware attacks etc.
- Investigate financial fraud and unauthorized transactions committed using digital resource.
- Assessing the effectiveness of its defences and incident response strategy whilst not limited to technical controls.
- Raising awareness of our security team's inherent strengths and weaknesses. This information will make informed decisions concerning Bank's security strategy.
- Helping the organization develop "battle-hardened" defences against Advanced Persistent Threats (APT), Ransomware etc.
- Testing the effectiveness of our Incident Response plans and challenge our team's breach detection capabilities.
- Assisting with identification of High Value Targets (HVTs) and weaknesses based on common methodologies. HVTs could be People, Systems, Processes or Technology.
- Provide assurance report to Bank that Bank is prepared/ready for Digital/Cyber Forensic Readiness covering all network and security devices, applications, concerned servers etc deployed in the Bank. This assurance has to be provided based on full assessment of Bank's network as per scope.

- Recommend improvements to security policies/cyber crisis plan based on forensic findings.

B) Scope for conduct of Cyber/Digital Forensic Incident Audit/ Investigation/ Analysis (but not limited to):

- Methodology for reporting findings of analysed data and making the information available for review through a secure online portal. The timeframe for storage of report findings to be mentioned.
- An end-to-end investigation tracks all elements of a suspected compromise, including how the compromise initiated, which devices/systems were compromised, and the associated recovery process.
- Should be able to provide cyber forensic services including (but not limited to) the examination of computers, mobile phones and other digital devices, digital evidence preservation, recovery, analysis, electronic mail extraction and database examination.
- Undertake Digital & Mobile Forensics including indexing of complete data, timeline analysis, meta data analysis, Decryption and password cracking, keyword searching, data retrieval etc.
- Perform Cyber forensic investigation of varied operating systems (but not limited to) Windows, Linux, UNIX, Mac OS, Enterprises OS etc.
- Perform Cyber forensics and Incident investigation of (but not limited to) web/client based applications, databases (Sybase, oracle, MS SQL, Postgress etc.)
- Perform cyber forensics and Incident investigation of (but not limited to) networking, email and security devices etc.
- To identify the malicious activities with respect to 5Ws + H (Why, When, Where, What, Who, How).
- Identify attack vectors by which a hacker (or cracker) could have gained access to a computer or network in order to deliver a payload or malicious outcome.
- Ensure that proper chain of custody (CoC) is maintained for integrity and all evidence recovery and collection methods are conducted, managed and achieved in a manner consistent to maintain preservation and protection of data and evidence in its original form such that it is admissible in the court of law.
- It is expected to retrieve information stored on the devices in a form useful to investigator during legal/cyber investigation and business exigency.
- Prepare and submit detailed forensic report on the technical and executive aspect of the investigation.
- Create and maintain an electronic audit trail or manual record of all processes, including work-papers, applied to gather and examine relevant evidences in such a way to ensure even third parties should be able to examine those processes and achieve the same result.
- Collection and Preservation of Electronic Evidence
- Data Recovery and Analysis
- Analysis of User/Malicious Activity
- Handling Password Protected Files
- Data Forensic Investigation
- Expert Testimony

- Secure Shipments, in case of need
- Chain of Custody Management
- Ability to meet the service levels.
- Ability and experience in providing IT Forensic and e-Discovery services to harvest data from IT security devices.
- Ability to provide services related to restoration of backup systems, including enterprise-wide backup systems.
- Ability to provide services related to restoration of corrupted, deleted, hidden, and encrypted or temporary data.
- Ability to provide services related to restoration of damaged media.
- Ability to provide services related to restoration of password protected files.
- Ability to have methodology for collecting data, including volatile data.
- Ability for preserving metadata during data capture with the goal of preserving the evidentiary value and the chain of custody.
- Conduct digital forensic analysis with various models, as and when incidents (which triggers forensic analysis as per the bank policy) happen.
- Methodology for analyzing preserved and collected data.
- Providing in detail the gaps in the existing security controls used to protect the data on banks premises and during transmission, transfer of Bank's data etc.
- Provide a sample of the types of logs that are created in the device throughout the review process and describe the process by which they are created.
- Detail the existing controls for secure transmission, transport, and shipment of Bank's data and your procedure used to protect the confidentiality and integrity of such data
- Information about the incident type and its modus operandi
- Description of how the incident was discovered.
- Information about the systems that were affected.
- Information about who was responsible for the system and its data.
- A description of what caused the incident.
- A description of the response to the incident and whether it was effective.
- Recommendations to prevent future incidents.
- A discussion on lessons learned to improve future responses.
- A timeline of events, from detection to incident closure
- Identify available sources of potential evidence in the environment, including: Email, Network traffic, logs, and archives, User documents, media, and voice mail, social media, Smart Mobile devices, Cloud Services, Smart devices, etc.
- Identify and validate the procedures carried out by IT team to securely gather legally admissible evidence to meet the Legal Regulatory requirements.
- A POC of replaying/reconstructing the same incident on test environment, proving the analysis is right.
- Reconstruct timelines and attack vectors, for demonstration to the Bank when necessary.
- Recover deleted, encrypted, or damaged data from Critical Systems including cloud (Private), when required by the Bank.

- Should support the Bank in identifying the attack simulations performed by the regulators and third-party vendors in the event of Cyber Drill Exercise.
- Must have the ability to perform malware analysis and reverse engineering of malware samples using both automated and manual techniques and provide host-based and network-based indicators that are used to find the malware variants.

The vendor should ensure that the following rules are upheld during an investigation:

- No possible evidence is damaged, destroyed, or compromised by the forensic procedures used to investigate the computer (preservation of evidence).
- No possible computer malware is introduced to the computer being investigated during the analysis process.
- Any extracted and possibly relevant evidence is properly handled and protected from later mechanical or electromagnetic damage (extraction and preservation of evidence).
- A continuing chain of custody is established and maintained (accountability of evidence).
- Normal operations are affected for a very limited period of time, if at all (limited interference of the crime scene on normal life).
- Details of the client-attorney relationship are not disclosed if obtained during a forensic process in order to maintain professional ethics and legality (ethics of investigation).

Vendor should guide electronic discovery and investigative processes, providing Bank's legal teams with sound advice and an expanded source of evidentiary techno legal information acceptable at judiciary platforms. Vendor should be able to carefully analyse the details of each case to conduct timely and thorough investigations to extract techno legal evidences acceptable at judiciary platforms.

The appointed vendor will conduct a desktop exercise upon appointment to guide bank stakeholders on the vital first steps to take during any incident.

The appointed Digital/Cyber Forensic vendor is expected to:

- Define the business scenarios that will require digital evidence collection.
- Reducing the impact of computer-related incidents.
- Guidance on ensuring compliance with regulatory or legal requirements.
- Determine evidence collection requirements and procedures.
- Establish evidence collection procedures that are legally admissible in court.
- Establish a policy for secure storage and handling of potential evidence.
- Facilitate training and understanding of security incidents and detection across the Bank network.
- Review and provide guidance within defined SLAs to reduce potential revenue losses and recovery of the same.
- Recommend changes to methodologies while minimizing negative customer impact.
- Represent the Bank in a court of law, as and when required, to substantiate their findings and provide supporting evidence and support Bank's legal council if necessary in this regards.

GeM Bid Ref: GEM/2025/B/6707442 **Date:** ***20.09.2025***

Broad Scope of work for RED TEAM EXERCISE:

I. BROADER PROJECT SCOPE:

- The Security Service Provider to conduct the Red Team Exercise to uncover the vulnerabilities in the bank's perimeter/ internal network (DC/ DR/NDR and on sample basis for branches/Offices and attempt to exploit the identified vulnerabilities to gain access to the bank's Critical Infrastructure like Servers, Databases, Network devices and Security Appliances.
- In order to enhance Information Security Posture of the Bank and to defend Bank against outside/internal threats Bank needs to carry out Red Team Exercise through the bidder to know various attack tactics and the methods to defend against such attacks.
- Red Teams will act proactively by simulating real attacks and attempt to penetrate security controls undetected. Their role is to highlight loopholes in Security Control and to improve detection, response, recovery and mitigation capabilities for Blue Team - SOC and IT operations.
- The impact on network performance should be minimal during Red Team Exercise and should not impact any normal user flows. Non-Destructive simulation Initiator would only be allowed to generate lightweight traffic. Tests in the production network should not be destructive - destructive behaviour tests are only done in the secure containers, a sandbox separated from the production network.
- The Red Team Exercise should provide information and guidance on remediation of identified results. The Red Team Exercise should provide ample information on the specifics of each attack in order to enable INDIAN BANK Security Operation Centre (SOC) Team and different other Teams (Network, Endpoint, Email, Data Centre, CBS etc.) to remediate any issues encountered.
- The Red Team Exercise should support testing email security controls against data exfiltration, malware, phishing etc.. It should enable the validation and tuning of INDIAN BANK's email security tools. It should leverage a dedicated internal and external email account destination to send threats like malware and spear-phishing links across the email server into INDIAN BANK, and to send sensitive information like PII and PCI data out of INDIAN BANK to validate that the email security and DLP controls in INDIAN BANK are in place are working as the Bank expects. This should support Office 365, Microsoft Exchange and other standard email Red Team Exercises.
- The Red Team Exercise should support executing external attacks from internet towards internal controls.
- The Red Team Exercise should support attack replay & attack import from PCA.
- Bidder is required to provide Red Team Exercise as a service only. However, required application, tools or any other appliance if required to conduct the Red Team Exercise to be arranged by the bidder at their own cost and to be deployed and used within the Bank's premises in presence of Bank Officials.

II. DETAILED SCOPE OF WORK

The Red team exercise should involve the full attack lifecycle, from initial reconnaissance to mission completion. The objective is to test and validate the ability to detect malicious activity and evaluate the response to the detected events. The Red team exercise should provide an accurate situational awareness of the security posture of a given system/network. The Red Teaming exercise must essentially include the undernoted phases:

Category	Activities
Reconnaissance	Passive scanning, OSINT gathering, domain enumeration, email harvesting
Initial Access	Phishing, watering hole attacks, exploiting public-facing apps, USB drops

Execution	PowerShell abuse, macro-enabled documents, scheduled tasks
Persistence	Registry run keys, startup folder implants, service creation
Privilege Escalation	Token manipulation, exploiting vulnerable drivers, bypassing UAC
Defence Evasion	DLL sideloading, obfuscation, disabling AV/EDR, clearing logs
Credential Access	LSASS dumping, keylogging, brute-force, credential spraying
Discovery	Network mapping, AD enumeration, identifying security controls
Lateral Movement	Pass-the-Hash, RDP hijacking, SMB exploitation, remote WMI
Collection	File scraping, clipboard monitoring, screen captures
Exfiltration	DNS tunnelling, HTTPS uploads, cloud sync abuse
Command & Control (C2)	Custom C2 frameworks, encrypted channels, domain fronting
Impact Simulation	Ransomware deployment (in isolated test), data corruption, service disruption

A. SCANNING PHASE :

i. Conduct ping sweep scans and identify the reachability of IP segments.
ii. Identify live IP addresses within the identified IP segments.
iii. Launch stealth/noisy scans on the bank's IP addresses and identify open & vulnerable ports.
iv. Intelligence gathering by Passive Reconnaissance to extract sub domains, hosts.
v. Identify IP ranges and vulnerabilities in publicly available server/network devices & internally.

B. FINGERPRINTING/ VULNERABILITY IDENTIFICATION PHASE.

i. Detecting TCP/UDP services and version details
ii. Detecting Operating systems and its version details using active and passive OS fingerprinting techniques without any impact on the production environment.
iii. Fingerprinting web servers and HTTP/ HTTPS services running on the bank's internal and external servers.
iv. Attempt to identify weakly configured web applications/ web servers/ Operating systems/ databases
v. Attempt to identify vulnerabilities in network services, operating systems, and Network devices using combination of advanced vulnerability scanners and manual tests.
vi. Script scan to identify potential vulnerabilities.
vii. Identify vulnerabilities in external facing web applications with Black Box approach.
viii. Identify potential exploits available for identified vulnerabilities using well known exploitation framework modules.

C. EXPLOITATION AND POST EXPLOITATION PHASE

This phase will include exploitation of the identified vulnerabilities in operating systems, web applications and network services. Post exploitation phase may include attempts to execute following key attacks in a controlled environment as applicable:

i. Gain access to the underlying operating system
ii. Evaluate the potential for gaining further access to the bank's internal network
iii. Extract credentials and password hashes from operating systems memory

iv. Exploiting OS misconfigurations and local process vulnerabilities to gain privileged access on target server

v. Attempt to identify if a device, web application is vulnerable to a default credential attack. vi. Attempt to exploit vulnerabilities in network/web services using exploitation frameworks and publicly available exploit codes as applicable.

vi. Examining Bank for weaknesses as through the eyes of an industrial spy or a competitor or attacker using following techniques:

a) Password Cracking, and Bypassing Windows User Account Control (UAC)
b) PowerShell exploitation, Pass the hash
c) Lateral Movement
d) Network Domination & Persistence
e) Network Infrastructure including end points and servers exploitation for cases such as Firewall bypass, Router testing/ configuration, DNS foot printing, Proxy Servers, Vulnerability exploits, Misconfiguration exploits
f) Evasion & Obfuscation Techniques
g) Data exfiltration - Internal network, External network, Storage device
h) Attacking Linux/Unix Environments
i) Privilege Escalation to obtain root privileges
j) Virtualization Attacks
k) Web application compromise and exploitation – physical and Cloud
l) Social Engineering Attacks (Spear phishing, Phishing,Vishing)
m) Carry out DDos attack exercise
n) Evade proxy rules
o) Covert channel call-backs
p) Local privilege escalation
q) Lateral network scans within and across subnets
r) Discover and access file shares
s) Horizontal brute force attacks
t) Brute force - Security appliances
u) Attempt to access - Remote branches, DMZ, Internal servers, Core Servers

D. SOCIAL ENGINEERING

Human interactions typically gain unauthorized access to systems or information that may result in system or network intrusion or disruption. The vendor shall be responsible for conducting social engineering attack (targeting employees through “Vishing” ,”Phishing” etc.) to assess the level of employee awareness in terms of cyber threats.

The common attack vectors include malicious emails, phone calls, removable media and physical penetration testing.

- ✓ External exposure of the Company
- ✓ Effectiveness of security awareness efforts
  - USB drop exercise
  - Through social media
  - Phishing
  - Vishing
  - SMShing etc.

E. TRAINING

Vendor is required to impart training to the identified bank personnel/ SOC team on the Red Team Exercise with use cases, analysis and resolution of the red team exercise carried out, functionality and services. In addition to that, mandatory training is to be provided to Bank staff yearly after completion of the activity for handling the guidance as Blue team against Red Team Exercise. Time to Detect & time to respond matrix should be prepared for the Bank to review the blue team performance.

F. RED TEAM ASSESSMENT

The Service Provider is required to deliver Red Team assessment with below specifications and actions:

a) Service Provider must use non-destructive methods necessary to accomplish a set of jointly agreed upon mission objectives while simulating attacker behaviour.
b) Scope of the assessment must cover the internal security team's ability to prevent, detect, and respond to incidents in a controlled and realistic environment against
   - Technology - Servers, Databases, Security & Networks, Applications, Routers, Switches, Appliances
   - People - Staff, Outsourced Vendor Personnel, Departments, business partners
   - Physical Facilities - Offices, Data Centre, Disaster Recovery Site
c) The Service Provider must closely mimic a real attacker's active and stealthy attack methods by using Technic, Tactics and Procedure (TTP) seen on real, recent incident response engagements in order to assess the security team's ability to detect and respond to an active attacker scenario. The service provider shall conduct red team exercise to focus on giving the bank's security teams a practical experience combating real cyber-attacks to simulate the tools, tactics and procedures (TTPs) of real world attackers that target our environment, while avoiding business damaging tactics.
d) Vendor must adopt fact-based risk analysis and recommendations approach.
e) The engagement must follow the phase of attack life cycle which minimally should consist of Initial Compromise, Establish Foothold, Lateral Movement, and Complete Mission.
f) Bidder must leverage a combination of proprietary intelligence repositories as well as industry leading commercial threat intelligence tools and techniques throughout the engagement.
g) The scope of engagement will include testing of the bank's detection and response capabilities.
h) From the samples provided, the bidder should be able to differentiate genuine and suspected fraudulent behaviour.
i) The red team exercise should cover a wide spectrum of applications, browsers, databases, web servers and other components.
j) Identify gaps in IT Perimeter security devices such as Firewall, WAF, NIPS, Proxy, EDR, HIPS and network segmentation.
k) ATM, Kiosk compromise simulation
l) Mobile App & Web portal attacks
m) Insider Threat Simulation
n) Swift Network Simulation
o) In case of each simulation, there should be feature for rollback wherever required.
p) Testing the incident response mechanism of the bank to identify the capability of the bank in breach readiness and thus Improve the organizational incident handling and recovery mechanism to 'restore the business in time' at the time of real cyber-attack.

q) Utilizing the existing security flaws to gather more information, owning the system, network, application etc.
r) Conducting controlled exercise to challenge the existing defending control system to get inside the organization by physically/logically/social means.
s) Should be able to demonstrate mitre attack framework to the Bank.

G. TOOLS

The service provider to ensure that the tools or any software used for conducting the assessment is fully licensed and property of the service provider. Any software or tool to be installed in any of the devices in Banks network or premises has to be done by the service provider by taking necessary permission and licenses, if any. The software or tools installed for the assessment have to be removed once the activity is over or the contract is terminated.

The necessary tool/software should be brought by the bidder installation in Bank's Premises only and should be customizable as per the scope of work.

Indicative list of custom attacks includes but not limited to:

- DNS requests
- Custom email (attachments, links in body, etc)
- Web requests
- Socket
- Host CLI for endpoint (python, bash, windows CMD, powershell)
- TCP Port Scan
- MITM attack (Man-in-the-middle)
- DNS redirection
- SQL Injection
- Web Defacement
- Password Brute Force
- Cross site scripting etc.

H. DELIVERABLES

The service provider should provide detailed test reports covering the following aspects at minimum:

- Executive summary
- Test methodology
- Observations
- Findings, Root causes
- Recommendations

After each Red Team Exercise, deliverables (supporting documents/ evidence) in relation to analysis should be reported/ submitted to the bank highlighting the findings and steps for mitigation of the same after completion of the exercise broadly covering the below aspects.

1. Detailing the Security Gaps:

Technical report of red team attack for each phase wise:

The deliverables need to include an electronic report that includes several key components, but not limited to:

- Control framework (i.e OWASP, PCI, PTES, OSSTMM).
- Summary of open-source intelligence (OSINT) gathered from internet and dark web
- Methodology and approach
- Target list created by OSINT
- Review of sensitive company data discovered on internet.
- Results of the assessment (description, business impact, recommendation, evidence, references, CVSS, risk rating, etc.)
- In addition to the electronic report, a raw file in comma-separated value (excel or CSV) format should also be provided in an effort to optimize the remediation and management of any identified findings.
- Detailing the System setup and tools used, and the tests conducted during the exercise.
- Analysis of the findings and document the security gaps such as vulnerability, configuration flaws, security flaws, gaps identified, threats etc. observed during the testing activity as per the scope of work.
- Document recommendations and Exercises for addressing the identified security gaps and categorize the identified security gaps based on their criticality.
- Chart a roadmap for the Bank to ensure compliance and address these security gaps.

2. Addressing the Security Gaps:

- Recommend actionable fixes for systems vulnerabilities in design or otherwise for application systems and network infrastructure. If recommendations for Risk Mitigation/ Removal could not be implemented as suggested after discussion with Bank, alternate compensatory controls to be provided.
- Suggest changes/modifications in the Security Policies implemented along with Security Architecture including Network and Applications of the Bank to address the same.

3. Summary of Final Report:

Summary of exercise findings including identification tests, tools used, and results of tests performed.

- Tools used and methodology employed.
- Positive security aspects identified.
- List of vulnerabilities identified with POC /supporting Evidences.
- Description of vulnerability
- Risk rating or severity
- Category of Risk: Critical / High / Medium / Low
- Methodology/Test cases used in exercises.
- Illustration of the test cases

4. Exit Meeting

Findings are to be communicated effectively in a stakeholder meeting and typically presented in person. During this time, red team security consultants should walk through the report, in detail to ensure all findings and their corresponding description, risk rating, impact, likelihood, evidence and remediation steps are thoroughly understood. While this typically involves a single meeting, there is no limitation to that number. The key aspect should be that all information is clearly understood and that a roadmap towards remediation/mitigation is clear.

After review, the service provider has to provide confirmation to the bank that functioning of network system is in compliance with

- Bank's Information Security Policy
- Bank's Cyber Crisis Management Plan
- RBI Information Security guidelines and Framework, CERT-In guidelines, any other legal requirements etc.

5. Remediation and re-testing

Remediation re-testing to be provided at no additional cost after compliance.

I. Systems presently prevailing in the Bank:

- Networks - Bank has a WAN setup connecting all the branches and offices PAN India using MPLS, VSAT, etc. The routers and switches used are of standard OEM models. The main core banking application is "Bancs". SWIFT application is also used in our setup. Delivery channels like ATMs (Onsite & Offsite), Internet & Mobile Banking, RTGS, NEFT, UPI and Financial Inclusion also form part of the network. Bank has major network and security solutions deployed in the network.

- People - Some of the IT operations are handled by Bank staff and some are outsourced to vendor personnel who are located in the premises within the Bank/Data Centre.

- Physical Facilities - Bank's Data Centre is located at third party Data Centre provider location. Our main IT department is located at Head Office in our own premises. Various other departments are also located in our own premises.

J. Other general requirements

The service provider should benchmark the policies, procedures/processes, standards against the standards recommended by RBI and identify gaps. The service provider should report on the areas where they have observed the bank to be non-compliant with the RBI guidelines.

The outcomes of the overall exercise should enable the bank to:

- Assess the effectiveness of its defenses and incident response strategy whilst not limited to technical controls.
- Provide a real-world cyber war/training opportunity and defend against a live attack.
- Raise awareness of our security team's inherent strengths and weaknesses. This information will make informed decisions concerning our security strategy.
- Help the organization develop defences against Advanced Persistent Threats (APT).
- Test the effectiveness of our incident response plans and challenge our team's breach detection capabilities.
- Assist with identification of High Value Targets (HVTs) and weaknesses based on common methodologies. HVTs could be People, Systems, Processes, Technology.

Broad scope of work for conducting Cyber Drill:

1. Purpose

The purpose of this engagement is to conduct a practical, hands-on cyber drill to test the bank's resilience to cyberattacks, identify gaps in its incident response capabilities, and enhance the technical skills of the security team. The ultimate goal is to validate and improve the bank's cyber security posture, ensuring full compliance with the regulatory Framework.

2. Phases of Engagement

Phase 1: Planning and Scenario Design

- Initial Consultation: The expert team will hold a kickoff meeting with key bank stakeholders to understand the current security landscape, existing controls, and specific concerns.
- Threat Scenario Development: The expert will design a realistic, multi-stage cyberattack scenario. This will not be a simple vulnerability scan but a narrative-driven attack, simulating initial compromise, lateral movement, and a final objective (e.g., data exfiltration or a financial system attack). The scenario will be tailored to the bank's environment and based on common threats in the financial sector.
- Rules of Engagement: A clear set of rules will be defined, outlining the scope, targets, and limitations of the drill to ensure no disruption to the bank's live production systems. The drill will be conducted in a controlled, isolated test environment.

Phase 2: Execution of the Drill

- Simulated Attack: The expert will execute the pre-designed scenario, acting as the "red team." This will involve using various techniques, including social engineering (e.g., simulated phishing), malware deployment in a test environment, and exploiting vulnerabilities to mimic a real attack.
- Active Defense: The bank's security team will act as the "blue team," using their existing tools and processes to detect, analyze, contain, and remediate the simulated threat. The drill will test their ability to identify IOCs (Indicators of Compromise), communicate effectively, and follow the pre-defined incident response plan.
- Observation and Data Collection: The expert will meticulously observe and document every step of the drill, logging the timeline of events, the actions of the blue team, and the effectiveness of security controls.

3. Deliverables

- Detailed Post-Drill Report: A comprehensive report will be provided, detailing the simulated attack timeline, a step-by-step breakdown of the blue team's response, and an analysis of their performance.
- Actionable Recommendations: The report will include a prioritized list of specific recommendations to improve the bank's cyber security. This will cover areas such as:
  - Process Improvements: Enhancements to the incident response plan, communication protocols, and a clear chain of command.
  - Technical Enhancements: Recommendations for new security tools, configuration changes, and patch management improvements.

- Skill Gaps: Identification of training needs for the security team to better handle future incidents.
- Executive Summary: A high-level, non-technical summary for senior management and the board, highlighting key findings, the bank's overall readiness score, and a high-level action plan.
- Debriefing Workshop: A formal debriefing session will be held with all stakeholders to review the findings, discuss the recommendations, and plan the next steps.

Broad Scope of work for Tabletop Exercise (TTX):

Tabletop Exercise will be simulated, discussion-based incident response activity where key stakeholders in the Bank will walk through a hypothetical crisis scenario like any cyberattack, data breach, natural disaster etc to test their response plans, communication protocols, and decision-making without real-world disruption or technical execution.

Walk the participants through the scenario step by step:

a) Initial Trigger – What event or situation initiates the need for change? (e.g., sudden failure, new regulation, etc.)

b) Impact Assessment – What are the potential impacts of this change across systems, teams, and processes?

c) Risk Assessment – What risks are involved, and how can they be mitigated?

d) Stakeholder Analysis – Who are the impacted stakeholders, and how will they be communicated with?

e) Plan Development – Tell participants to draft elements of the CCMP (timelines, roles, resources, communication).

f) Execution and Monitoring – How will the change be implemented, and how will it be monitored?

g) Post-Implementation Review – What metrics will be used to assess the success of the change?

Tabletop assessment will be for following scenarios (but not limited to):

a) Ransomware

b) Compromise of Critical System

c) DOS & DDOS Attacks

d) Data Breach/ Leakage/ Exfiltration (external)

e) Malware attack at critical setup like DC/DRS

f) Defacement of websites

g) Third party service provider compromised

h) Crown Jewel IT Asset corrupted/ failed

i) Major failures of Network at DC/DRS

Primary Objectives of a Tabletop Exercise:

a) Validate Incident Response Plans

b) Clarify Roles and Responsibilities and Confirm that each participant (technical, legal, PR, HR, etc) understands their duties during an incident.

c) Test internal communication channels and escalation processes across teams and different departments.

d) Improve Decision-Making Under Pressure

e) Identify Gaps in People, Processes or Technology

f) Test Regulatory and Legal Readiness

g) Assess how the organization handles breach notification, compliance and interaction with regulators or law enforcement agency.

h) Increase Organizational Awareness and Resilience in operation and technology

2) Period of Validity of Bids

Bids should remain valid for the period of 180 days after the last date for submission of bid prescribed by the Bank. A bid valid for a shorter period shall be rejected by the Bank as non-responsive. Bank may seek extension of bid validity period, if required.

3) Authorization to Bid

Responses submitted by a Bidder to this RFP (including response to functional and technical requirements) represent a firm offer to contract on the terms and conditions described in the tender document. The proposal must be signed by an official authorized to commit the bidder to the terms and conditions of the proposal. Bidder must clearly identify the full title and authorization of the designated official and provide a statement of bid commitment with the accompanying signature of the official and submit the copy of power of attorney/ authority letter authorizing the signatory to sign the bid.

4) Timeframe for completion of activities

Bidder shall be responsible for the complete delivery, installation, implementation and maintenance of the services as per the timelines mentioned in the table below. Any breach in the timelines shall lead to imposition of penalty.

S.No.	Milestone	Timeline
1.	Incident Response Readiness Assessment (IRRA)	Within 60 days from date of Purchase Order
2.	Cyber/Digital Forensic Readiness Assessment	Within 60 days from date of Purchase Order
3.	Review of Incident reporting mechanism of Bank	Within 60 days from the date of Purchase Order

4.	Red Team Exercise	Within 1 year from the date of Purchase Order
5.	Tabletop Exercise	Within 1 year from the date of Purchase Order
6.	Cyber Drill	Within 1 year from the date of Purchase Order
7.	NDA/SLA/Contract execution	Within 30 days from the date of Purchase Order

8.	**Incident Response services initiation timelines**:		
	S.No.	Initial response 24*7*365 days support facility for incident response	Upper time limit
	1.	Incident's initial response and containment once alerted from Bank through call/email/message/any other communication medium for any location.	4 hrs
	2.	Once the incident is confirmed, the IR analyst must start working on preliminary information submitted by the Bank IR support.	6 hrs
	3.	Onsite location support – Incident response analyst should be available in the location of incident whenever needed	
	3.1	Within Tier -1 cities, metro cities & state capitals of India	12 hrs
	3.2	Within India- Other than above mentioned cities in 3.1	24 hrs
9.	**Incident resolution and restoration timelines:** 1. Critical Incidents must be resolved within 02 days. 2. High Severity Incidents must be resolved within 04 days. 3. Medium Severity Incidents must be resolved within 07 days. 4. Low severity incidents must be resolved within 10 days. 5. For specific type of incidents such as ransomware attack, data breach and phishing attack shall be decided, defined & mutually agreed between Bank and Bidder in the SLA.		
10.	IR support vendor shall submit comprehensive incident report within 24 hours from incident resolution & restoration to Bank.		

*Immediate remedial action should be taken upon flagging of observations / vulnerabilities having critical and high rating without waiting for final report.

5) Payment Terms

1.	**Payment schedule**	**On completion of Incident Response Readiness Assessment (IRRA) (i.e., Phase 1):** Payment would be made against raising of invoices, along with submission of all relevant documents or deliverables.
		On completing Incident Response Process: On actual deployment/usage of IR services, an invoice for actual Hours/Man-day utilized for incident response can be processed

		upon satisfactory completion of each incident response.
2.	**Payment schedule**	**On completion of Digital/Cyber Forensic Readiness Assessment:** Payment would be made against raising of invoices, along with submission of all relevant documents or deliverables.
		On completing Cyber/Digital Forensics Incident Audit / Investigation / Analysis: On actual deployment/usage of Forensic services, an invoice for actual Hours/Man-days utilized can be processed upon satisfactory completion of each case.
3.	**Payment schedule**	**On completion of Red Team Exercise, Tabletop Exercise and Cyber Drill**: Payment would be made against raising of invoices, along with submission of all relevant documents or deliverables.

***** Payment will be made yearly in arrears, after completion (on acceptance by Bank) of services.

Note:

I. TDS on payments will be deducted as applicable.
II. All the payments will be made to bidder electronically in Indian Rupees only. Payment will be made against delivery invoices and challans duly acknowledged by Bank officials.
III. Further, the above payments will be released only after submission of Accepted copy of Purchase Order, Performance Bank Guarantee, signing of SLA & NDA, Integrity pact by Successful Bidder.
IV. No advance payment will be made.
V. All the payments to the Bidder shall be subject to the report of satisfactory accomplishment of the concerned task / performance/ delivery of the Services to the satisfaction of Bank for this purpose.
VI. Penalties if any, on account of non-compliance of Service Requirements/ liquidated damages, if any, shall be deducted from the invoice value/ EMD amount.
VII. Under no circumstances Bank shall be liable to the Successful Bidder and/or its employees/personnel/representatives/agent etc. for direct, indirect, incidental, consequential, special or exemplary damages arising from termination of the Contract.
VIII. Bank shall not have any liability whatsoever in case of any third-party claims, demands, suit, actions or other proceedings against the Successful Bidder or any other person engaged by the Successful Bidder in the course of performance of the Service.
IX. Bank reserves the rights to dispute/deduct payment/withhold payments/further payment due to the Successful Bidder under the Contract, if the Successful Bidder has not performed or rendered the Services in accordance with the provisions of the Contract which the Bank at its sole discretion adjudge.

X. Successful Bidder shall permit Bank to hold or deduct the amount from invoices, for non-performance or part performance or failure to discharge obligations under the Contract.

XI. It is clarified that any payments of the charges made to and received by Successful Bidder personnel shall be considered as a full discharge of Bank's obligations for payment under the Agreement.

XII. All out of pocket expenses, travelling, boarding and lodging expenses for the entire Term of this RFP and subsequent agreement is included in the amounts quoted in TCO and the Bidder shall not be entitled to charge any additional costs on account of any items or services or by way of any out-of-pocket expenses, including travel, boarding and lodging.

XIII. In case Bank extends Contract period, the tenure of the existing Performance Bank Guarantee shall have to be extended accordingly for the duration of contract extension and claim period of an additional 6 months. In case the same is not feasible due to any reason, Bidder shall have to submit a Performance Bank Guarantee of the same amount (10% of the Total Cost of Ownership) as submitted previously for the duration of contract extension and claim period of an additional 6 months.

6) Service Level Agreement (SLA)

The Bidder shall have to enter into an agreement with Bank as per the terms and conditions of this RFP and it's subsequent Corrigendum/ Corrigenda.

The non-delivery of services or non-response or any breach of information will lead to penalty. The penalty is applicable in respect of non-delivery of services/ support as per the requirement of this RFP.

Within **30 days** of receipt of the Order/Letter of Intent, the selected Bidder shall sign and date, the Service Level Agreement (SLA), on stamp paper of appropriate value, in format of the Bank and return it to Bank. The Bidder, however, may submit the SLA Form they like to execute. It is prerogative of the Bank to accept the same or to modify. It is reiterated that the Contract/SLA to be entered into by the Selected Bidder shall be as approved by the Bank only. Bank expects that the Bidder shall be bound by the Service Levels described in this document.

S.No.	Milestone	Frequency	Timeline	Penalty
1.	Incident Response Readiness Assessment (IRRA)	Annual	Completion of milestone within 90 days from the date of instruction from the Bank.	Penalty of Rs.5000 Per Day will be applicable, in case of delay.
2.	Cyber/Digital Forensic Readiness Assessment	Annual	Completion of milestone within 90 days from the date of instruction from the Bank.	Penalty of Rs.5000 Per Day will be applicable, in case of delay.

3.	Incident Response Support and Reporting	On Demand	RCA, Cyber Forensic report etc. to be submitted within 15 days, post reporting of incidence	Penalty of Rs.25000 Per Day will be applicable, in case of delay.
4	Cyber / Digital Forensics incident Audit / Investigation / Analysis and Reporting	On Demand	RCA, Cyber Forensic report etc. to be submitted within 15 days, post reporting of incidence	Penalty of Rs.25000 Per Day will be applicable, in case of delay.
4.	Red Team Exercise	Annual	Completion of milestone within 90 days from the date of instruction from the Bank.	Penalty of Rs.5000 Per Day will be applicable, in case of delay.
5.	Tabletop Exercise	Annual	Completion of milestone within 60 days from the date of instruction from the Bank.	Penalty of Rs.5000 Per Day will be applicable, in case of delay.
6.	Cyber Drill	Annual	Completion of milestone within 60 days from the date of instruction from the Bank.	Penalty of Rs.5000 Per Day will be applicable, in case of delay.

	Incident Response services initiation timelines:			**Penalty**
7	S.No.	Initial response 24*7*365 days support facility for incident response	Upper time limit	Penalty of Rs.10,000/- Per hour will be applicable, in case of delay.
	1.	Incident's initial response and containment once alerted from Bank through call/email/message/any other communication medium for any location and confirmation of incident.	4 Hrs.	
	2.	Once the incident is confirmed, the IR analyst must start live response analysis working on preliminary information submitted by the Bank IR support.	6 Hrs.	

	3.	Onsite location support – Incident response analyst should be available in the location of incident wherever needed		
	3.1	Within Tier -1 cities, metro cities & state capitals of India	12 Hrs. (Excluding travel time)	
	3.2	Within India- Other than above mentioned cities in 3.1	24 Hrs. (Excluding travel time)	
9.	**Incident resolution and restoration timelines:** 1. Critical Incidents must be resolved within 02 days, 2. High Severity Incidents must be resolved within 04 days. 3. Medium Severity Incidents must be resolved within 07 days. 4. Low severity incidents must be resolved within 10 days. 5. For specific type of incidents such as ransomware attack, data breach and phishing attack shall be decided, defined & mutually agreed between Bank and Bidder in the SLA. Criticality of incident will be decided mutually between Bank and Successful Bidder.			Penalty of Rs. 5,000/- Per Day will be applicable, in case of delay.
10.	IR support vendor shall submit comprehensive incident report within 24 hours from incident resolution & restoration to Bank.			Penalty of Rs. 5,000/- Per Day will be applicable, in case of delay.

7) Contract Period

The Period of contract will be Three (3) years from the date of acceptance of purchase order.

8) Sub-Contracting

The successful bidder will not subcontract or delegate or permit anyone other than the bidders' personnel to perform any of the work, service or other performance required of the supplier under this agreement without the prior written consent of the Bank. Sub-Contracting is not allowed, however, Bank at its own discretion may permit or deny the same.

9) Governing language

The contract and all correspondence/ communications and other documents pertaining to the Contract, shall be written in English.

10) Insurance

The goods supplied under the Contract shall be fully insured against loss or damage incidental to transportation, storage, and erection. The transit insurance shall be for an amount equal to 110 percent of the invoice value of the Goods from "Warehouse to final destination" on "All Risks" basis including War Risks and Strikes. In case the successful bidder is covering the goods under a Master Policy, bidder has to submit a declaration along with copy of master insurance stating that all the items are covered under the said master policy. If insurance policies for transit insurance & storage & erection is not provided, then 10% of the warranty invoice value will be deducted from the payment for each insurance policy not submitted by bidder.

11) Jurisdiction and Applicable Law

The Contract shall be interpreted in accordance with the laws of India. Any dispute arising out of this contract will be under the jurisdiction of Courts of Law in Chennai. Compliance with labour and tax laws, etc. will be the sole responsibility of the supplier/ service provider at their cost.

12) Liquidated Damages (LD)

If the Supplier fails to deliver any or all of the Goods/Services or to perform the Services within the period(s) specified in the order, for reasons solely attributable to the Supplier, or the goods fail to perform to desired efficiency/ standards/ functionalities, then Purchaser shall, deduct from the relevant order price, as liquidated damages, Rs.10,000/- for the delayed Goods/ Services for each day or part thereof of delay until actual delivery/completion of services, up to a maximum deduction of 10% of the total cost outlay of respective services for a period of three years. Once the maximum is reached, the Purchaser may consider termination of this order.

13) Bank's right to accept or reject any bid or all bids

- The Bank reserves the right to accept or reject any bid / all bids or annul the bidding process at any time prior to awarding the contract, without thereby incurring any liability to the affected Bidder or Bidders.

- Bank reserves the right to modify the terms and conditions of this RFP duly informing the same before due date of submission of bids & publishing the same on Bank Website and GeM portal.

14) Performance Security

a. Within 15 days of issue of Purchase Order, the successful bidder shall furnish to the Bank the Performance Security equivalent to 5% of the contract value in the form of a Bank Guarantee from a scheduled commercial Bank located in India, valid for **36 months** with further **3 months** claim period, in the format enclosed (Annexure-IV). Relaxation if any, extended by GOI/ competent authorities for furnishing PBG shall be passed on to eligible bidders.

b. The performance security submitted by the successful bidder shall be invoked by the Bank as compensation for any loss resulting from the bidder's failure in completing their obligations or any other claim under the Contract.

c. The performance security will be discharged by the Bank and returned to the successful bidder not later than thirty (30) days following the date of completion of the successful performance obligations under the Contract.

d. Failure of the successful bidder to comply with the requirement of signing of contract and providing performance security shall constitute sufficient grounds for annulment of the award and forfeiture of the bid security, in which event the Bank may call for new bids

15) Limitation of Liability

Successful bidders' aggregate liability under the contract shall be at actual and limited to a maximum of the contract value. For the purpose for the section, contract value at any given point of time, means the aggregate value of the purchase orders placed by bank on the vendor that gave rise to claim, under this tender.

This limit shall not apply to third party claims for

a. IP Infringement indemnity

b. Bodily injury (including death) and damage to real property and tangible property caused by vendor' or its employee/ agents.

If a third party asserts a claim against bank that a vendor product acquired under the agreement infringes a patent or copy right, vendor should defend the bank against that claim and pay amounts finally awarded by a court against bank or included in a settlement approved by vendor**.**

16) Indemnity Clause

If at the time of the supplying the goods or services or installing the platform/ software in terms of the present contract/ order or subsequently it appears at any point of time that an infringement has occurred of any right claimed by any third party in India or abroad, then in respect of all costs, charges, expenses, losses and other damages which the Bank may suffer on account of such claim, the supplier shall indemnify the Bank and keep it indemnified on that behalf.

17) Disclaimer

The Bank and/or its officers, employees disown all liabilities or claims arising out of any loss or damage, whether foreseeable or not, suffered by any person acting on or refraining from acting because of any information including statements, information, forecasts, estimates or projections contained in this document or conduct ancillary to it whether or not the loss or damage arises in connection with any omission, negligence, default, lack of care or misrepresentation on the part of Bank and/or any of its officers, employees.

This RFP is not an agreement by the Authority to the prospective Bidders or any other person. 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 in preparation or submission of the Bid, regardless of the conduct or outcome of the Bidding Process.

The information contained in this RFP document, or any information provided subsequently

to Bidder(s) whether verbally or in documentary form by or on behalf of the Bank, is provided to the Bidder(s) on the terms and conditions set out in this RFP document and all other terms and conditions subject to which such information is provided.

This RFP is neither an agreement nor an offer and is only an invitation by Bank to the interested parties for submission of bids. The purpose of this RFP is to provide the Bidder(s) with information to assist in the formulation of their proposals. This RFP does not claim to contain all the information each bidder may require. Each Bidder should conduct its own investigations and analysis and should check the accuracy, reliability and completeness of the information in this RFP and where necessary, obtain independent advice. Bank makes no representation or warranty and shall incur no liability under any law, statute, rules or regulations as to the accuracy, reliability or completeness of this RFP.

This is not an offer by the Bank but only an invitation to bid in the selection process initiated by the Bank. No contractual obligation whatsoever shall arise from the RFP process until a formal contract is executed by the duly authorized signatory of the Bank and the Bidder.

18) Patent Rights

The Supplier shall indemnify the Bank against all third-party claims of infringement of patent, trademark or industrial design rights arising from use of the Goods or software or hardware or any part thereof. In the event of any claim asserted by the third party of infringement of copyright, patent, trademark or industrial design rights arising from the use of the Goods or any part thereof, the bidder shall act expeditiously to extinguish such claims. If the bidder fails to comply and Bank is required to pay compensation to a third party resulting from such infringement, the bidder shall be responsible for the compensation including all expenses, court costs and lawyer fees. Bank will give notice to the bidder of such claims, if it is made, without delay by fax/e-mail/registered post.

19) IT Act 2000

The equipment's to be quoted as per this tender should comply with the requirements under Information Technology (IT) Act 2000 and subsequent amendments and related Government/Reserve Bank India guidelines issued from time to time.

20) Intellectual Property Rights (IPR)

While the successful bidder/ OEM shall retain the intellectual property rights for the application software, it is required that successful bidder shall grant user-based annual subscription License to the bank for the bank's exclusive use without limitation on the use of those licenses. The successful bidder shall place the source code of customizations done for the bank in Banks environment (and the procedures necessary to build the source code into executable form) for the application software, and the source code of the application software in escrow with a reputable agency (a bank or established software escrow firm in India) acceptable to the Bank during the contract period.

Notwithstanding the disclosure of any confidential information by the disclosing party to the receiving party, the disclosing party shall retain title and all intellectual property and

proprietary rights in the confidential information. No License under any trademark, patent or copyright or application for same which are or thereafter may be obtained by such party is either granted or implied by the conveying of confidential information.

Bidder warrants that the inputs provided and/or deliverables supplied by them does not and shall not infringe upon any third-party intellectual property rights, including copyrights, patents and other intellectual property rights of any nature whatsoever.

In the event that the Deliverables become the subject of claim of violation or infringement of a third party's intellectual property rights, bidder shall at its choice and expense: [a] procure for Bank the right to continue to use such deliverables; [b] replace or modify such deliverables to make them non-infringing, provided that the same function is performed by the replacement or modified deliverables as the infringing deliverables; or [c] if the rights to use cannot be procured or the deliverables cannot be replaced or modified, accept the return of the deliverables and reimburse the bank for any amounts paid to bidder for such deliverables, along with the replacement costs incurred by Bank for procuring an equivalent equipment in addition to the penalties levied by Bank. However, Bank shall not bear any kind of expense, charge, fees or any kind of costs in this regard. Notwithstanding the remedies contained herein, the bidder shall be responsible for payment of penalties in case service levels are not met because of inability of the bank to use the proposed product.

The indemnification obligation stated in this clause apply only in the event that the indemnified party provides the indemnifying party prompt written notice of such claims, grants the indemnifying party sole authority to defend, manage, negotiate or settle such claims and makes available all reasonable assistance in defending the claims [at the expenses of the indemnifying party. Notwithstanding the foregoing, neither party is authorized to agree to any settlement or compromise or the like which would require that the indemnified party make any payment or bear any other substantive obligation without the prior written consent of the indemnified party. The indemnification obligation stated in this clause reflects the entire liability of the parties for the matters addressed thereby.

The bidder acknowledges that business logics, workflows, delegation and decision-making processes of Bank are of business sensitive nature and shall not be disclosed/referred to other clients, agents or distributors.

21) Acceptance of Purchase Order

Acceptance of purchase order should be submitted within 7 days of issuance of purchase order along-with authorization letter by the successful bidder to the Bank. If for any reason successful bidder backs out after issuance of purchase order or the purchase order issued to the successful bidder does not get executed in part / full, Bank shall invoke performance bank guarantee and blacklist the bidder for a period of one year.

22) Signing of Contract Form, NDA, SLA and Submission of Undertaking of Labour Law Compliance

Within twenty-one (21) days from the date of Purchase Order, the successful bidder shall sign the contract form (Annexure-III), Non-Disclosure Agreement (Annexure-VI) and

Service Level Agreement (Annexure-XX) and return it to the Bank. Pre-Contract Integrity Pact (Annexure-V) executed between the Bank and successful bidder(s) is deemed to be a part of the contract. Penalties will be pegged at the rate of 10,000/- per day for delay in the submission of documents.

Successful bidder has to submit the Undertaking of Labour Law Compliance (Annexure-X).

23) Settlement of Disputes

a. If any dispute or difference of any kind whatsoever shall arise between the Bank and the supplier in connection with or arising out of the contract, the parties shall make every effort to resolve amicably such dispute or difference by mutual consultation.

b. If the parties fail to resolve their disputes or difference by such mutual consultation within a period of 30 days, then either the Bank or the supplier may give notice to the other party of its intention to commence arbitration, as hereinafter provided, as to the matter in dispute, and no arbitration in respect of this matter may be commenced unless such notice is given.

Any dispute or difference in respect of which a notice of intention to commence arbitration has been given in accordance with this clause shall be finally settled by arbitration. Arbitration may be commenced prior to or after delivery of the goods under the contract. Arbitration proceedings shall be conducted in accordance with the following rules of procedure.

The dispute resolution mechanism to be applied shall be as follows:

a) In case of dispute or difference arising between the Purchaser and a Supplier relating to any matter arising out of or connected with the agreement, such dispute or difference shall be settled in accordance with the Arbitration and Conciliation Act, 1996. The arbitral tribunal shall consist of 3 arbitrators one each to be appointed by the Purchaser and the Supplier; the third Arbitrator shall be chosen by the two Arbitrators so appointed by the Parties and shall act as Presiding Arbitrator. In case of failure of the two arbitrators appointed by the parties to reach upon a consensus within a period of 30 days from the appointment of the presiding Arbitrator, the Presiding Arbitrator shall be appointed by the Indian Banks' Association, India which shall be final and binding on the parties.

b) If one of the parties fails to appoint its arbitrator within 30 days after receipt of the notice of the appointment of its Arbitrator by the other party, then the Indian Banks' Association shall appoint the Arbitrator. A certified copy of the order of the Indian Banks' Association making such an appointment shall be furnished to each of the parties.

c) Arbitration proceedings shall be held at Chennai, India, and the language of the arbitration proceedings and that of all documents and communications between the parties shall be English.

d) The decision of the majority of arbitrators shall be final and binding upon both parties. The cost and expenses of Arbitration proceedings will be paid as determined by the Arbitral Tribunal. However, the expenses incurred by each party in connection with the preparation, presentation etc. of its proceedings as also the fees and expenses paid to the arbitrator appointed by such party or on its behalf shall be borne by each party itself.

e) Where the value of the contract is Rs. 10 million and below, the disputes or differences arising shall be referred to the Sole Arbitrator. The Sole Arbitrator shall be appointed by agreement between the parties; failing such agreement, by the appointing authority namely the Indian Banks' Association (IBA).

f) Notwithstanding any reference to arbitration herein,

a. the parties shall continue to perform their respective obligation under the contract unless they otherwise agree; and

b. the Bank shall pay the supplier any monies due to the supplier.

Submitting to arbitration may be considered as an additional remedy and it does not preclude Parties to seek redressal/ other legal recourse.

24) Exit Requirements

In the event, the Agreement between the Bank and the Successful bidder comes to an end on account of termination or by the expiry of the term / renewed term or otherwise, the Supplier shall render all reasonable assistance and help to the Bank and to any new vendor engaged by the Bank, for the smooth switch over and continuity of the Services.

25) Termination for Convenience

The Bank, with 90 days' written notice sent to the Successful bidder, may terminate the Contract, in whole or in part, at any time for its convenience. The notice of termination shall specify that termination is for the bank's convenience, the extent to which the performance of the Successful bidder under the Contract is terminated, and the date upon which such termination becomes effective.

The Goods that are complete and ready for shipment within ninety (90) days (period can be fix as per project requirement) after the Supplier's receipt of notice of termination shall be accepted by the Purchaser at the Contract terms and prices. For the remaining Goods, the Purchaser may elect:

a. to have any portion completed and delivered at the Contract terms and prices; and / or

b. to cancel the remainder and pay to the Supplier an agreed amount for partially completed Goods and Services and for materials and parts previously procured by the Supplier.

26) Termination for Default

The Bank, without prejudice to any other remedy for breach of contract, by 90 days' written notice of default sent to the Supplier, may terminate this Contract in whole or in part:

a. if the successful bidder fails to deliver any or all of the Goods and Services within the period(s) specified in the Contract, or within any extension thereof granted by the Purchaser.

b. if the successful bidder fails to perform any other obligation(s) under the Contract.

c. If the successful bidder, in the judgement of the Purchaser, has engaged in corrupt or fraudulent practices in competing for or in executing the Contract.

d. In case of successful Bidders revoking or cancelling their Bid or varying any of the terms in regard thereof without the consent of the Bank in writing.

'For the purpose of this clause:

"corrupt practice" means the offering, giving, receiving or soliciting of anything of value to influence the action of a public official in the procurement process or in contract execution; and

"**fraudulent practice**" means a misrepresentation of facts in order to influence a procurement process or the execution of a contract to the detriment of the Bank and includes collusive practice among Bidders (prior to or after bid submission) designed to establish bid prices at artificial non-competitive levels and to deprive the Bank of the benefits of free and open competition.

In the event the Bank terminates the Contract in whole or in part, the Bank may procure the Goods or Services similar to those undelivered, upon such terms and in such manner as it deems appropriate, and the Supplier shall be liable to the Bank for any excess costs paid/ to be paid by the Bank for such similar Goods or Services. However, the Supplier shall continue performance of the Contract to the extent not terminated.

27) Force Majeure

The Successful bidder shall not be liable for forfeiture of its performance security, liquidated damages, or termination for default, if and to the extent that, its delay in performance or other failure to perform its obligations under the Contract is the result of an event of Force Majeure. For purposes of this clause, "Force Majeure" means an event beyond reasonable control of the Successful bidder and not involving the Successful bidder's fault or negligence and not foreseeable. Such events may include, but are not restricted to, acts of the Bank in its sovereign capacity, wars or revolutions, fires, floods, epidemics, quarantine restrictions, and freight embargoes. Delay by sub suppliers of vendor to Vendor will not be considered as cause of force Majeure.

If a Force Majeure situation arises, the Successful bidder shall promptly notify the Bank in writing of such condition and the cause thereof but in any case, not later than 10 (Ten)

days from the moment of their beginning. Unless otherwise directed by the Bank in writing, the Successful bidder 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.

If the impossibility of complete or partial performance of an obligation lasts for more than 6 (six) months, either party hereto reserves the right to terminate the contract totally or partially upon giving prior written notice of 30 (thirty) days to the other party of the intention to terminate without any liability other than reimbursement on the terms provided in the agreement for the goods received or complete transition / handover to the in-coming Vendor / Service Provider**.**

28) Termination of Services/ Contract

Bank shall serve the notice of termination to the successful bidder at least 30 days prior, of its intention to terminate services. The Bank will be entitled to terminate the services/ contract, without any cost to the Bank and recover expenditure incurred by Bank, on the happening of any one or more of the following:

a. The successful bidder commits a material breach of any of the terms and conditions of the bid.
b. The successful bidder goes into liquidation voluntarily or otherwise. In such case, the source code, and other developments in software, etc. will become proprietary of the Bank.
c. An attachment is levied or continues to be levied for a period of 7 days upon effects of the Agreement.
d. The progress regarding the execution of the order accepted by the successful bidder is found to be unsatisfactory or delay in execution of the contract, the Bank reserves the right to get the balance contract executed by another party of its choice by giving one month's notice for the same. In this event, the successful bidder is bound to make good the additional expenditure, which Bank may have to incur in executing the balance contract. This clause is applicable, if for any reason, the contract is cancelled.
e. Non-satisfactory performance of the successful bidder during implementation and operation.
f. An act of omission by the Bidder, its employees, its agents, or employees of the consortium in the performance of the services provided by this contract.
g. Failure to integrate/implement the Project as per the requirements of the Bank as stated in this RFP.
h. Material discrepancies in the Deliverables and Services noted in the implementation of the Project. Bank reserves the right to procure the same or similar product from the alternate sources at the risk, cost and responsibility of the bidder.
i. Successful bidder is found to be indulged in frauds.
j. The bank suffers a reputation loss on account of any activity of successful bidder or penalty is levied by regulatory authority.
k. In the event of subcontract or assignment contrary to the terms of agreement.
l. In the event of termination of the project specific contract.

29) Confidentiality

The supplier will be exposed to internal business information of the Bank, affiliates, and / or business partners by virtue of the contracted activities. The Bidder / their employees shall treat all data & information collected from the Bank during the project in strict confidence. The Bank is expected to do the same in respect of Bidder provided data / information. ***After termination of the contract also the successful bidder / supplier shall not divulge any data/ information collected from the Bank during the project.***

During the expiry or termination of the contract, the successful bidder shall handover the complete data related to the project, to the Bank in a manner specified by the Bank. The successful bidder shall also provide all support for migrating the data from the successful bidder's system to the new system, to be implemented by the Bank or the new service provider of the Bank, at no additional cost to the Bank.

The supplier will have to enter into a Non-Disclosure agreement (Annexure-VI) with the Bank to safeguard the confidentiality of the Bank's business information, legacy applications and data.

The successful bidder and its employees either during the term or after the expiration of the contract shall not disclose any proprietary or confidential information relating to the project, the services, the contract, or the business or operations without the prior written consent of the Bank.

The successful Bidder and its employees shall not publish or disclose in any manner, without the Bank's prior written consent, the details of any security safeguards designed, developed, or implemented by the successful Bidder under this contract or existing at any Bank location. The successful Bidder shall develop procedures, and implementation plans to ensure that IT resources leaving the control of the assigned user (such as being reassigned, removed for repair, replaced, or upgraded) are cleared of all Bank data and sensitive application software. The successful Bidder shall also ensure that all permitted subcontractors who are involved in providing such security safeguards or part of it shall not publish or disclose in any manner, without the Bank's prior written consent, the details of any security safeguards designed, developed, or implemented by the successful Bidder under this contract or existing at any Bank location.

30) Negligence

If the successful bidder neglects to execute the work with due diligence or expedition or refuses or neglects to comply with any reasonable order given in writing by the Bank in connection with the work or contravenes the provisions of other Terms, in such eventuality, the Bank may after giving notice in writing to the successful bidder calling upon him to make good the failure, neglect or contravention complained of, within such times as may be deemed reasonable and in default of the said notice, the Bank shall have the right to cancel the Contract holding the successful bidder liable for the damages that the Bank may sustain in this behalf. Thereafter, the Bank may make good the failure at the risk and cost of the successful bidder.

31) Amalgamation

If the Bank undergoes a merger, amalgamation, take-over, consolidation, reconstruction, change of ownership etc., this RFP shall be considered to be assigned to the new entity and such an act shall not affect the obligations of the successful bidder under this RFP. In such case, decision of the new entity will be binding on the successful bidder.

32) Software/Hardware requirements

All the software, hardware equipment like Laptops, tools etc. to carry out the assignment has to be brought by the selected Bidder at no extra cost to the Bank.

33) Substitution of Project Team Members

During the assignment, the substitution of key staff identified for the assignment will not be allowed by the Bank unless such substitution becomes unavoidable to overcome the undue delay or that such changes are critical to meet the obligation. In such circumstances, the selected Bidder, as the case may be, can do so only with the prior written concurrence of the Bank and by providing the replacement staff of the same level of qualifications and competence. If the Bank is not satisfied with the substitution, the Bank reserves the right to terminate the contract and recover whatever payments made by the Bank to the selected Bidder during the course of the assignment pursuant to this RFP besides claiming an amount equal to the contract value as liquidated damages. However, the Bank reserves the unconditional right to insist to the selected Bidder to replace any team member with another member (with the qualifications and competence as required by the Bank) during the course of assignment pursuant to this RFP.

34) Use of Contract Documents and Information

The successful bidder shall not, without the Purchaser's prior written consent, disclose the Contract, or any provision thereof, or any specification, plan, drawing, pattern, sample or information furnished by or on behalf of the Purchaser in connection therewith, to any person other than a person employed/authorized by the successful bidder in the performance of the Contract. Disclosure to any such employed/authorized person shall be made in confidence and shall extend only so far as may be necessary for purposes of such performance.

The successful bidder shall not, without the Purchaser's prior written consent, make use of any document or information pertaining to this contract except for purposes of performing the Contract.

35) Pre-Contract Integrity Pact

Bidders shall submit Pre-Contract Integrity Pact (IP) along with the technical bid as per Annexure-V of the RFP. Pre-Contract Integrity Pact is an agreement between the prospective bidders and the Bank committing the persons/officials of both the parties not to exercise any corrupt influence on any aspect of the contract. Any violation of the terms of Pre-Contract Integrity Pact would entail disqualification of the bidders and exclusion from future business dealings.

The Pre-Contract Integrity Pact begins when both parties have legally signed it. Pre-Contract Integrity Pact with the successful bidder(s) will be valid till 12 months after the last payment made under the contract. Pre-Contract Integrity Pact with the unsuccessful bidders will be valid till 6 months after the contract is awarded to the successful bidder.

Adoption of Pre-Contract Integrity Pact

- The Pact essentially envisages an agreement between the prospective bidders and the Bank, committing the persons /officials of both sides, not to resort to any corrupt practices in any aspect/ stage of the contract.
- Only those bidders, who commit themselves to the above pact with the Bank, shall be considered eligible for participate in the bidding process.
- The Bidders shall submit signed Pre-Contract integrity pact as per the Annexure-V. Those Bids which are not containing the above are liable for rejection.
- Foreign Bidders to disclose the name and address of agents and representatives in India and Indian Bidders to disclose their foreign principles or associates.
- Bidders to disclose the payments to be made by them to agents/brokers or any other intermediary. Bidders to disclose any transgressions with any other company that may impinge on the anti-corruption principle.
- Pre-Contract Integrity Pact in respect this contract would be operative from the stage of invitation of the Bids till the final completion of the contract. Any violation of the same would entail disqualification of the bidders and exclusion from future business dealings.
- The Pre-Contract Integrity Pact Agreement submitted by the bidder during the Bid submission will automatically form the part of the Contract Agreement till the conclusion of the contract i.e. the final payment or the duration of the Warranty /Guarantee/AMC if contracted whichever is later.
- Integrity Pact, in respect of a particular contract would be operative from the stage of invitation of bids till the final completion of the contract. Any violation of the same would entail disqualification of the bidders and exclusion from future business dealings.
- Pre-Contract Integrity Pact shall be signed by the person who is authorized to sign the Bid.
- The Name and Contact details of the Independent External Monitor (IEM) nominated by the Bank are as under:

1. Shri. Mohan J Joseph
   Email: mohan.joseph@gmail.com

- Any Change in law / policy / circular relating to Pre-Contract Integrity Pact which vitiate the agreement shall accordingly be applicable with immediate effect on written intimation from the Bank.

- Any violation of Pre-Contract Integrity Pact would entail disqualification of the bidders and exclusion from future business dealings, as per the existing provisions of GFR, 2017, Prevention of Corruption Act (PC Act), 1988 or other Financial Rules as may be applicable to the Bank.

36) Implementation of Services

The successful bidder shall provide all the services specified hereunder having Technical and Functional specifications in accordance with the highest standards of professional competence and integrity. If the Bank finds that any of the staff of the successful bidder assigned to work at the Bank's site is not responsive, then the successful bidder will be notified accordingly and the successful bidder shall be under obligation to resolve the issue expeditiously to the satisfaction of the Bank.

37) Termination for Insolvency

If the successful bidder becomes bankrupt or insolvent, has a receiving order issued against it, compounds with its creditors, or, if the successful bidder is a corporation, a resolution is passed or order is made for its winding up (other than a voluntary liquidation for the purposes of amalgamation or reconstruction), a receiver is appointed over in part of its undertaking or assets, or if the successful bidder takes or suffers any other analogous action in consequence of a debt; then the Bank may at any time terminate the contract by giving a notice to the successful bidder.

If the contract is terminated by the Bank in terms of this clause, termination will be without compensation to the successful bidder 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.

In case the termination occurs before implementation of the project/ delivery of goods/services in full, in terms of this clause, the Bank is entitled to make its claim to the extent of the amount already paid by the Bank to the successful bidder.

38) Taxes and Duties

The successful bidder shall be liable to pay all taxes that shall be levied against it, in accordance with the laws applicable from time to time in India.

39) Compliance with Policy

The successful bidder shall have to comply with Indian Bank's policies like IT policy, Information Security policy, Cyber Security Policy, Digital Personal Data Protection Policy etc. in key concern areas relevant to the RFP, details of which shall be shared with the successful bidder.

40) Compliance with Statutory and Regulatory Provisions

The successful bidder shall comply with all statutory and Regulatory provisions while executing the contract awarded by Bank.

41) Other Terms and Conditions

- The relationship between the Bank and Successful Bidder/s is on principal-to-principal basis. Nothing contained herein shall be deemed to create any association, partnership, joint venture or relationship or principal and agent or master and servant or employer and employee between the Bank and Successful Bidder/s hereto or any affiliates or subsidiaries thereof or to provide any party with the right, power or authority, whether express or implied to create any such duty or obligation on behalf of the other party.

- Successful bidder/Service Provider shall be the principal employer of the employees, agents, contractors, subcontractors etc., engaged by the successful bidder/Service Provider and shall be vicariously liable for all the acts, deeds, matters or things, of such persons whether the same is within the scope of power or outside the scope of power, vested under the contract. No right of any employment in the Bank shall accrue or arise, by virtue of engagement of employees, agents, contractors, subcontractors etc., by the successful bidder/Service Provider, for any assignment under the contract. All remuneration, claims, wages dues etc., of such employees, agents, contractors, subcontractors etc., of the successful bidder/Service Provider shall be paid by the successful bidder/Service Provider alone and the Bank shall not have any direct or indirect liability or obligation, to pay any charges, claims or wages of any of the successful bidder's/Service Provider's employees, agents, contractors, subcontractors etc. The Successful Bidder/Service Provider shall agree to hold the Bank, its successors, assigns and administrators fully indemnified, and harmless against loss or liability, claims, actions or proceedings, if any, whatsoever nature that may arise or caused to the Bank through the action of Successful Bidder/Service Provider's employees, agents, contractors, subcontractors etc.

42) GENERAL TERMS AND CONDITIONS

42.1 Rejection of Bids

The Bank reserves the right to reject the Bid if,

i. Bidder does not meet any of the pre-bid eligibility criteria mentioned above including non-payment of the bid cost.
ii. The bid is incomplete as per the RFP requirements.
iii. Any condition stated by the bidder is not acceptable to the Bank.
iv. If the RFP and any of the terms and conditions stipulated in the document are not accepted by the authorized representatives of the bidder.
v. Required information not submitted as per the format given.
vi. Any information submitted by the bidder is found to be untrue/fake/false.

vii. The bidder does not provide, within the time specified by the bank, the supplemental information / clarification sought by the bank for evaluation of bid.

The Bank shall be under no obligation to accept any offer received in response to this RFP and shall be entitled to reject any or all offers without assigning any reason whatsoever. The Bank may abort entire process at any stage without thereby incurring any liability to the affected Bidder(s) or any obligation to inform the affected Bidder(s) of the grounds for Bank's action.

In order to promote consistency among the Proposals and to minimize potential misunderstandings regarding how Proposals will be interpreted by the Bank, the format in which Bidders will specify the fundamental aspects of their Proposals has been broadly outlined in this RFP.

Any clarifications to the RFP should be sought by email as per the dates mentioned in **"Schedule [A] Important Dates"**. Bank will hold a pre-bid meeting, to answer all the questions / queries received by email which would also be uploaded on bank's website and GeM portal.
Proposals received by the Bank after the specified time and date shall not be eligible for consideration and shall be summarily rejected.

In case of any change in timeline, the same shall be updated on the Bank's website and shall be applicable uniformly to all bidders.

42.2 Representation and Warranties

The Bidder represents and warrants as of the date hereof, which representations and warranties shall survive the term and termination hereof, the following:

i. That the representations made by the Bidder in its Bid are and shall continue to remain true and fulfil all the requirements as are necessary for executing the duties, obligations and responsibilities as laid down in the RFP and unless the Bank specifies to the contrary, the Bidder shall be bound by all the terms of the RFP.

ii. That all the representations and warranties as have been made by the Bidder with respect to its Bid and Contract, are true and correct, and shall continue to remain true and correct through the term of this Contract.

iii. That the execution of the Services herein is and shall be in accordance and in compliance with all applicable laws.

iv. That there are –
   (a) No legal proceedings pending or threatened against Bidder or any sub Bidder/third party or its team which adversely affect/may affect performance under this Contract; and

(b) no inquiries or investigations have been threatened, commenced or pending against Bidder or any sub-Bidder / third part or its team members by any statutory or regulatory or investigative agencies.

v. That the Bidder is validly constituted and has the corporate power to execute, deliver and perform the terms and provisions of this Contract and has taken all necessary corporate action to authorize the execution, delivery and performance by it of the Contract.

vi. That all conditions precedent under the Contract has been complied by the bidder.

vii. That neither the execution and delivery by the Bidder of the Contract nor the Bidder's compliance with or performance of the terms and provisions of the Contract:

a) will contravene, any provision of any applicable law or any order, writ, injunction or decree of any court or government authority binding on the Bidder,
b) will conflict or be inconsistent with or result in any breach of any or the terms, covenants, conditions or provisions of, or constitute a default under any agreement, contract or instrument to which the Bidder is a Party or by which it or any of its property or assets is bound or to which it may be subject, or
c) Will violate any provision of the Memorandum or Articles of Association of the Bidder.

viii. That the Bidder certifies that all registrations, recordings, filings and notarizations of the bid documents/ agreements/ contract and all payments of any tax or duty, including without limitation stamp duty, registration charges or similar amounts which are required to be effected or made by the Bidder which is necessary to ensure the legality, validity, enforceability or admissibility in evidence of the Contract have been/ shall be made.

ix. That the Bidder confirms that there has not and shall not occur any execution, amendment or modification of any agreement/contract without the prior written consent of the Bank, which may directly or indirectly have a bearing on the Contract or the project.

x. That the Bidder owns or has good, legal or beneficial title, or other interest inthe property, assets and revenues of the Bidder on which it grants or purports to grant or create any interest pursuant to the Contract, in each case free and clear of any encumbrance and further confirms that such interests created or expressed to be created are valid and enforceable.

xi. That the Bidder owns, has license to use or otherwise has the right to use, free of any pending or threatened liens or other security or other interests all

Intellectual Property Rights, which are required or desirable for the project and the Bidder does not, in carrying on its business and operations, infringe any Intellectual Property Rights of any person. None of the Intellectual Property or Intellectual Property Rights owned or enjoyed by the Bidder or which the Bidder is licensed to use, which are material in the context of the Bidder's business and operations are being infringed nor, so far as the Bidder is aware, is there any infringement or threatened infringement of those Intellectual Property or Intellectual Property Rights licensed or provided to the Bidder by any person. All Intellectual Property Rights (owned by the Bidder or which the Bidder is licensed to use) are valid and subsisting. All actions (including registration, payment of all registration and renewal fees) required by the bidder to maintain the same in full force and effect have been taken thereon and shall keep the Bank indemnified in relation thereto.

xii. Any intellectual property arising during the course of the execution under the contract related to tools/ systems/ product/ process, developed with the consultation of the bidder will be intellectual property of the Bank.

42.3 Relationship of Parties

i. Nothing in the Contract shall constitute any fiduciary relationship between the Bank and Bidder/Bidder's Team or any relationship of employer – employee, principal and agent, or partnership, between Indian Bank and Bidder and /or its employees.
ii. No Party has any authority to bind the other Party in any manner whatsoever, except as agreed under the terms of the Contract.
iii. Indian Bank has no obligation to the successful Bidder, except as agreed under the terms of the Contract.
iv. All employees/personnel/ representatives/agents etc., engaged by the Successful Bidder for performing its obligations under the Contract/RFP shall be in sole employment of the Successful Bidder and the Successful Bidder shall be solely responsible for their salaries, wages, statutory payments etc. Under no circumstances, shall Indian Bank be liable for any payment or claim or compensation (including but not limited to any compensation on account of any injury / death / termination) of any nature to the employees/personnel/representatives/agent etc. of the Successful Bidder.
v. Supplier/Vendor has to take an undertaking from their employees connected with the contract/RFP/solution to maintain the confidentiality of the Bank's information/documents etc. Bank may seek details / confirmation on background verification of Vendor's employees worked/working on Bank's project as may have been undertaken / executed by the Vendor, Vendor should be agreeable for any such undertaking/verification.
vi. The Successful Bidder shall disclose to Indian Bank in writing, all actual and potential conflicts of interest that exist, arise or may arise (either for the Successful Bidder or its team/agents/representatives/personnel etc.) in the course of performing the Services as soon as practical after it becomes aware of that conflict.
vii. The Successful Bidder shall not make or permit to be made a public announcement or media release about any aspect of the Bid/ Contract unless Indian Bank first gives the Successful Bidder its prior written consent.

42.4 No Right to Set Off

In case the Successful Bidder has any other business relationship with the Bank, no right of set-off, counter-claim and cross-claim and or otherwise will be available under the agreement to the said Bidder for any payments receivable under and in accordance with that business.

42.5 Publicity

Any publicity by the Bidder in which the name of the Bank is to be used should be done only with the explicit written permission of the Bank.

42.6 Conflict of Interest

The Bidder shall disclose to the Bank in writing, all actual and potential conflicts of interest that exist, arise or may arise (either for the Bidder or the Bidder's team) in the course of performing the services / appointment as soon as practical after it becomes aware of that conflict.

42.7 Solicitation of Employees

The selected Bidder, during the term of the contract shall not without the express written consent of the Bank, directly or indirectly:

a) recruit, hire, appoint or engage or attempt to recruit, hire, appoint or engage or discuss employment with or otherwise utilize the services of any person who has been an employee or associate or engaged in any capacity, by the Bank in rendering services in relation to the contract; or

b) induce any person who shall have been an employee or associate of the Bank at any time to terminate his/ her relationship with the Bank.

42.8 Notices and Other Communication

If a notice has to be sent to either of the parties following the signing of the contract, it has to be in writing and shall be sent personally or by certified or registered post with acknowledgement due or overnight courier or email duly transmitted, addressed to the other party at the addresses, email given in the contract.

Notices shall be deemed given upon receipt, except that notices sent by registered post in a correctly addressed envelope shall be deemed to be delivered within 5 working days (excluding Sundays and public holidays) after the date of mailing dispatch and in case the communication is made by email, on business date immediately after the date of successful email. (that is, the sender has a hard copy of the page evidencing that the email sent to correct email address).

Any Party may change the address, email address and fax number to which notices are to be sent to it, by providing written notice to the other Party in one of the manners provided in this section.

42.9 Severability

If any provision herein becomes invalid, illegal or unenforceable under any law, the validity, legality and enforceability of the remaining provisions and this RFP shall not be affected or impaired.

SECTION - IV

INSTRUCTIONS TO BIDDERS FOR ONLINE TENDER THROUGH GeM PORTAL

1.1. SUBMISSION OF BIDS THROUGH GeM PORTAL

The Bid documents, to be uploaded as part of online bid submission, are as follows:

a. Eligibility Criteria, along with all supporting documents required.

b. All Annexures as per this tender on Bidder's letter head with authorizing person's signature and Bidder seal on all pages.

c. All supporting documents and product literature in support of Technical/ Functional specifications.

d. Relevant brochures

f. Compliance to Technical/ Functional Specifications as per Technical Bid.

g. Any other information sought by the Bank with relevant to this tender.

Bidder should upload all the copies of relevant documents without fail in support of their bid and as per the instructions given in tender documents. If the files to be uploaded are in PDF format, ensure to upload it in "Searchable" PDF Format. After filling data in predefined forms bidders need to click on final submission link to submit their encrypted bid.

Please take care to scan documents so that total size of documents to be uploaded remains minimum. Unless specified in this RFP, **every document submitted online to the Bank shall be in PDF Format. The Scanned Documents shall be OCR enabled for facilitating "search" on the scanned document.** Utmost care may be taken to name the files/documents to be uploaded on e-tendering portal.

1.2. BID RELATED INFORMATION

Bidders must ensure that all documents uploaded on e-tendering portal as files or zipped folders, contain valid files and are not corrupt or damaged due to any processing at bidder PC system like zipping etc. It shall be the responsibility of bidder themselves for proper extractability of uploaded zipped files.

Any error/virus creeping into files/folder from client end PC system cannot be monitored by e-tender software/server and will be bidder's responsibility only.

1.3. OFFLINE SUBMISSIONS

In addition to uploading the documents in our e-Tendering portal, Bidders should also submit the following in a sealed envelope, super scribing with the tender Reference number, last date and time of bid submission, Name of the Bidder, etc.

a) Bid Security (EMD) in the form of DD/ Fund transfer/ Bank Guarantee (issued by a nationalised / scheduled commercial Bank (other than Indian Bank) in favour of "Indian Bank" payable at Chennai.

b) Pre-Contract Integrity Pact

Note: Companies registered as Micro/Small Units under MSE/NSIC should submit documentary proof for claiming exemption from Cost of Bid document.

The bidder is requested to submit the original documents (as mentioned under point no. 8 of Schedule [A]) in a Sealed Envelope on or before ***13.10.2025 03:00 PM*** to the address mentioned under point no. 4 of [A] (Important Dates and Information on RFP Submission) of schedule of this tender. The envelope shall be super scribed as "**Request for Proposal for Selection and Appointment of service provider for Incident Response (IR), Cyber/Digital forensic services, Red Team, Tabletop & Cyber Drill Exercise**" and the words '**DO NOT OPEN BEFORE 13.10.2025 03:30 PM**.

1.4. OTHER INSTRUCTIONS

For further instructions like system requirements and manuals, the bidder should visit GeM portal or banks Website.

GeM Bid Ref: GEM/2025/B/6707442 **Date:** ***20.09.2025***

SECTION-V

PART I - Technical and Functional Requirements

Date:

The Asst. General Manager
Indian Bank
Information System Security Department
Ground Floor
66, Rajaji Salai,
Chennai – 600 001

Dear Sir,

Sub: Request for Proposal for Selection and Appointment of service provider for Incident Response (IR), Cyber/Digital forensic services, Red Team, Tabletop & Cyber Drill Exercise.

Ref: Your RFP No. GEM/2025/B/6707442 dated 20.09.2025

******

Referring to your above RFP, we submit the compliance details of the specifications given below:

Technical BID - Technical and Functional Specification Compliance

S/N	Applicable Service	Description	Requirement (Mandatory(M) / Desirable(D)	Compliance (Y/N)
1	**Incident Response** **Cyber Forensics**	Service provider must have at least 5 years of experience in incident response and forensic investigations related to Cyber Security incidents in Information Technology Infrastructure, across various countries (at least 5 countries).	M	
2	**Incident Response** **Cyber Forensics**	Service provider must have deep knowledge of attack methodologies, background, objectives, target countries/verticals categorized by specific APT groups, especially Threat event occurrences in Asia-India Region and in financial sector around the globe.	M	
3	**Incident Response Cyber Forensics**	Service provider must release at least 5 reports, media articles, whitepapers on topics related cyber security, information security, attack vectors etc.	D	

4	**Incident Response** **Cyber Forensics**	Service provider must use combination of their own tools, scripts, inbuilt tools in available in Operating system wherever applicable to perform the incident response and forensic investigation in order to collect telemetry data across Perimeter, Network & Endpoint and collaborate.	D	
5	**Incident Response** **Cyber Forensics** **Red Team Exercise** **Cyber Drill**	The tools used by Service provider must commercially license with proper entitlement.	M	
6	**Incident Response** **Cyber Forensics** **Red Team Exercise**	The tools used by Service provider must support telemetry data collections from IT Networks / Systems / Endpoints.	M	
7	**Incident Response** **Cyber Forensics**	If required, the service provider must have the ability to perform malware analysis and reverse engineering of malware samples using both automated and manual techniques and provide host-based and network-based indicators that are used to find the malware variants in the wild.	M	
8	**Incident Response** **Cyber Forensics**	As part of the engagement, the service provider shall support in all subsequent phases of DFIR lifecycle – triage/analysis, containment, eradication and recovery, and post- incident review.	M	
9	**Cyber Forensics**	The service provider shall be equipped with tools and processes to ensure chain of custody is maintained throughout the engagement, secure handling and secure disposal of evidence (upon completion of assessment).	M	
10	**Incident Response** **Cyber Forensics**	Extensive library of latest file hashes and Indicators of Compromise (IOC) and Threat Intelligence should be maintained utilised during assessment to analyse network traffic, servers, PCs, network devices, and critical log data during assessment.	D	

	Cyber Drill			
11	**Incident response** **Cyber Forensics**	Service provider must have in-house capabilities or past experience to engage with law enforcement agencies and CERTs of different countries to aid in investigations. Public reference on case studies of your engagement with law enforcement agencies shall be provided.	M	
12	**Incident Response** **Cyber Forensics** **Red Team Exercise** **Cyber Drill**	The Service provider must be recognized by the industry experts and listed minimum once in last three year, in external market research reports published by Forrester Wave, Gartner's Magic Quadrant, or International Data Corporation (IDC), AiteNovarica, IT Central Station etc. for their DF/IR/RedTeam/Cyber Drill services.	D	
13	**Incident Response** **Cyber Forensics**	The Service provider must have responded to more than 100 cyber security incidents in last 5 years globally, out of which at least 10 percent belongs to DFIR in BFSI sector.	M	
14	**Incident Response** **Cyber Forensics** **Red Team Exercise** **Cyber Drill**	The Service provider must have cumulative experience of 10000 hours in last three year in DF/IR/Red Team/Cyber Drill engagements.	M	
15	**Incident Response**	The Service provider may have more than 25 MITRE Attack references.	D	
16	**Incident Response**	The Service provider must be able to provide profiles of at least 10 Advanced Persistent Threat (APT) / Threat Actor groups with comprehensive insights built based on tracking-of and responding to threats/breaches originating from these APT groups.	M	

17	**Incident Response**	The endpoint agent/EDR/solution which bidder is using during assessment/incident response, must be installed and monitored in at least One Million Endpoints / Honeypots / Sensors globally.	D	
18	**Incident Response** **Cyber Forensics** **Red Team Exercise** **Cyber Drill**	The Service provider must have dedicated team of more than 100 Security Researchers, Analysts, and Incident Responders.	M	
19	**Incident Response** **Cyber Forensics** **Red Team Exercise** **Cyber Drill**	At least three (3) relevant client references for DF/IR/RedTeam/Cyber Drill shall be provided, for each reference include (client name may be redacted to comply with NDA); • Nature of the engagement, dates of the engagement, • Name (or description) of the client firm, and a summary of the activities Bidder performed. • If necessary, references can be interviewed via blind conference calls to protect Bidder's previous clients' confidentiality.	M	
20	**Incident Response** **Cyber Forensics**	Provide DFIR engagements has Bidder had in the past three (3) years involving APT group intrusions. Provide examples of the nature of the intrusion and major activities that Bidder performed, or consulted with the customer organization to perform, in the past three (3) to remediate the intrusion.	M	
21	**Incident Response** **Cyber Forensics**	Provide redacted DFIR engagements has Bidder had in the past three (3) years involving ransomware attacks. Provide examples of the nature of the intrusion and major activities that Bidder has performed.	M	
22	**Incident Response** **Cyber Forensics**	Provide the experience Bidder's analysts have with malware analysis along with the tools used for DFIR.	M	

23	**Incident Response** **Cyber Forensics** **Red Team Exercise** **Cyber Drill**	Provide five (5) sample resumes that represent a typical team. Names of the individuals are not necessary.	M	
24	**Incident Response** **Cyber Forensics** **Red Team Exercise** **Cyber Drill**	Bidder should have experience presenting information about incidents to a Board of Director level body. Provide details of Bidder's staff has this type of experience.	M	
25	**Incident Response** **Cyber Forensics** **Red Team Exercise** **Cyber Drill**	Provide at least three (3) sample (redacted) final report for DF/IR/Red Team/Cyber Drill engagement.	M	
26	**Cyber Forensics**	The bidder shall submit minimum 3 evidence (client name may be redacted to comply with NDA) in last 5 years, confirming that the forensic work conducted is legally admissible in a court of law and supports the client's case.	M	
27	**Red Team Exercise**	The bidder's team includes certified ethical hackers with recognized certifications (e.g., OSCP, CREST).	M	
28	**Red Team Exercise** **Cyber Drill**	The scope of testing is clearly defined and approved by the organization before commencement.	M	
29	**Red Team Exercise**	The attack simulation uses advanced tools and techniques to mimic real-world adversaries.	M	
30	**Red Team Exercise** **Cyber Drill**	The testing is conducted without disrupting critical business operations.	M	

31	**Red Team Exercise** **Cyber Forensics** **Cyber Drill**	A detailed report is provided post-exercise highlighting vulnerabilities, exploited vectors, and remediation advice.	M	
32	**Red Team Exercise** **Cyber Drill**	Testing scenarios are customized based on the organization's infrastructure and threat landscape.	M	
33	**Red Team Exercise** **Cyber Drill**	Evidence and logs from testing are securely collected and stored for review.	M	
34	**Incident Response** **Cyber Forensics** **Red Team Exercise** **Cyber Drill**	The bidder guarantees confidentiality and enforces non-disclosure agreements.	M	
35	**Red Team Exercise** **Cyber Drill**	The exercises include follow-up support for remediation activities if required.	D	
36	**Tabletop Exercise**	The bidder conducts facilitated, scenario-based tabletop exercises led by experienced moderators.	M	
37	**Tabletop Exercise**	Scenarios are tailored to the specific cyber risks and organizational context of the client.	M	
38	**Tabletop Exercise**	Clear objectives and expected outcomes are established before the exercise.	M	
39	**Tabletop Exercise**	The exercise is structured within a predefined environment to simulate real-time decision-making.	M	
40	**Tabletop Exercise**	The process includes documenting lessons learned and recommended improvements to incident response plans.	M	
41	**Cyber Drill** **Tabletop Exercise**	The bidder provides a post-exercise (planned) debrief report summarizing findings and suggested actions.	M	

42	**Cyber Drill** **Tabletop Exercise**	The bidder can simulate comprehensive cyber attack scenarios across networks, applications, and endpoints.	M	
43	**Cyber Drill**	The exercise includes multiple attack vectors such as malware, phishing, social engineering, and external intrusions.	M	
44	**Cyber Drill**	The drill assesses the effectiveness of incident detection, response, and recovery procedures.	M	
45	**Cyber Drill**	Simulated threat intelligence feeds and attack techniques are used to mimic realistic threats.	M	
46	**Cyber Drill**	The organization receives a comprehensive post-drill report with findings, gaps, and recommendations.	M	

For

Office Seal
Place:
Date:

(Authorised Signatory)
Name:
Designation:
Mobile No:
Business Address:

Telephone No:
E-mail ID:

GeM Bid Ref: GEM/2025/B/6707442 **Date:** ***20.09.2025***

PART – II

Commercial Bid

(Price bid along with Breakup to be submitted with Technical Bid)

Date:

The Asst. General Manager
Indian Bank
Information System Security Department
Ground Floor
66, Rajaji Salai,
Chennai – 600 001

Dear Sir,

Sub: Request for Proposal for Selection and Appointment of service provider for Incident Response (IR), Cyber/Digital forensic services, Red Team, Tabletop & Cyber Drill Exercise.

Ref: Your RFP No. GEM/2025/B/6707442 dated 20.09.2025

We submit hereunder the price breakup details for Incident Response & Cyber/Digital Forensic, Red Team Exercise, Tabletop Exercise and Cyber Drill Services as per the specifications.

(To be filled by the Bidder – All amounts in INR, inclusive of taxes)

Sl. No.	Service Component	Unit	Year 1 Cost (INR) (a)	Year 2 Cost (INR) (b)	Year 3 Cost (INR) (c)	Total Cost (INR) – Excluding Tax (d)= (a)+(b)+(c)	Applicable Taxes (INR) (e)	Total Cost for 3 Years (INR) – Including Taxes (f)=(d)+(e)	Remarks
1	Incident Response Readiness Assessment	Annual							One per year
2	Cyber/Digital Forensic Readiness Assessment	Annual							One per year

3	On-demand Incident Response Support	15 man-days**						man-days = working of one person for one day
4	On-demand Cyber/Digital Forensic Audit / Investigation / Analysis	15 man-days**						man-days = working of one person for one day
5	Red Team Exercise	Annual						One per year
6	Cyber Drill	Annual						One per year
7	Tabletop Exercise	Annual						One per year
Grand Total (Fixed + Minimum Mandatory Activities)								

** man-days = working of one person for one day

Amount in Words (inclusive of all Taxes):_____

Instructions for Bidders:

1. Prices shall remain firm for 3 years.
2. All-inclusive pricing (travel, lodging, licenses, manpower, reports, documentation).
3. Unit rates (for incidents/forensics) will remain fixed for 3 years.
4. Applicable TDS or any taxes, if any, will be deducted from the payment.
5. Commercial Bid should be strictly in the above format only. No additional conditions should be included in the Bill of Material.
6. Bidder has to quote Total Cost of the project (inclusive of taxes) for three years while submitting its quote in GeM portal. Bank will consider the quote manually entered in GeM portal only.
7. In case of discrepancy between unit price and Total price, the unit price shall prevail.
8. The Unit and Total Cost should be given in full INR (i.e. without decimal places). All payments will also be in INR.

GeM Bid Ref: GEM/2025/B/6707442 **Date:** ***20.09.2025***

9. If a technically qualified bidder does not participate in the reverse auction process, Bank will consider the commercial price submitted by the bidder in GeM portal (while submitting technical bid) for the purpose of commercial evaluation.
10. The Bank reserves the right to negotiate line-item rates if required.
11. Rates quoted will remain valid for the entire contract duration (including extensions, if any).

We submit that we shall abide by the details given above and the conditions given in your above Bid document.

For

Office Seal
Place:
Date:

(Authorised Signatory)
Name:
Designation:
Mobile No:
Business Address:
Telephone No:
E-mail ID:

GeM Bid Ref: GEM/2025/B/6707442 **Date:** ***20.09.2025***

(LIST OF ANNEXURES)

ANNEXURE-I

Bid Form

(Bidders are required to furnish the Bid Form on its letter head)

Date: _____

To

The Asst. General Manager
Indian Bank
Information System Security Department
Ground Floor
66, Rajaji Salai,
Chennai – 600 001

Dear Sirs,

Sub: Request for Proposal for Selection and Appointment of service provider for Incident Response (IR), Cyber/Digital forensic services, Red Team, Tabletop & Cyber Drill Exercise.

Ref: Your RFP No. GEM/2025/B/6707442 dated 20.09.2025

Having examined the Bidding Documents, the receipt of which is hereby duly acknowledged, we, the undersigned, offer to..... ..... (Description of Goods and Services), in conformity with the said Bidding Documents.

We undertake, if our bid is accepted, to deliver the goods & services in accordance with the delivery schedule specified in the Schedule of Requirements.

If our bid is accepted, we will obtain the Guarantee of a Bank in a sum equivalent to 5% per cent of the Contract Price for the due performance of the Contract, in the form prescribed by the Bank.

We agree to abide by this for the bid validity period specified and it shall remain binding upon us and may be accepted at any time before the expiration of that period. We agree to extend the Bid Validity Period, if required.

Until a formal contract is prepared and executed, this bid, together with your notification of award, shall constitute a binding Contract between us.

We further represent and warrant that, the representations and warranties specified in under RFP document has been read and understood by us and we agree that they shall survive the term and termination.

GeM Bid Ref: GEM/2025/B/6707442 **Date:** ***20.09.2025***

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.

We understand that you are not bound to accept the lowest or any bid you may receive.

We confirm that we comply with the qualification criteria of the bidding documents and are submitting proof of the same along with bid.

Dated this .....day of ..... 2025.

Signature .....

.....
(In the Capacity of)

Duly authorised to sign bid for and on behalf of

(Name & Address of Bidder)

.....

.....

.....

Mobile:

Email

GeM Bid Ref: GEM/2025/B/6707442 **Date:** ***20.09.2025***

ANNEXURE-II

Self-Declaration – Blacklisting

The Asst. General Manager
Indian Bank
Information System Security Department
Ground Floor
66, Rajaji Salai,
Chennai – 600 001

Dear Sir,

Sub: Request for Proposal for Selection and Appointment of service provider for Incident Response (IR), Cyber/Digital forensic services, Red Team, Tabletop & Cyber Drill Exercise.

Ref: Your RFP No. GEM/2025/B/6707442 dated 20.09.2025

We hereby certify that, we have not been blacklisted by any Government Dept. / PSUs / Banks/ PSBs / Financial Institutions currently.

Signature of Authorized Official

Name and Designation with Office Seal

Place:

Date:

GeM Bid Ref: GEM/2025/B/6707442 **Date:** ***20.09.2025***

ANNEXURE–III

Contract Form

(To be submitted on Non - Judicial Stamp Paper)

THIS AGREEMENT made the .....day of.....2025 Between Indian Bank, having its Head Office, Information System Security Department, 66 Rajaji Salai, Chennai - 600001 (hereinafter "the Purchaser") which term shall unless repugnant to the context or meaning thereof shall mean its successors and assigns) of the one part and …… (Name of Supplier) having its Registered Office at …… (City and Country of Supplier) (hereinafter called "the Supplier") which term shall unless repugnant to the context or meaning thereof shall mean its successors and permitted assigns) of the other part:

WHEREAS the Purchaser invited bids vide RFP No. ……. for **Selection and Appointment of service provider for Incident Response (IR), Cyber/Digital forensic services, Red Team, Tabletop & Cyber Drill Exercise** (Brief Description of Goods and Services) and has accepted a bid by the Supplier for the provision of those goods and services in the sum for .... (Contract Price in Words and Figures) (hereinafter called "the Contract Price").

NOW THIS AGREEMENT WITNESSETH AS FOLLOWS:

1. In this Agreement words and expressions shall have the same meanings as are respectively assigned to them in the Conditions of Contract referred to.

2. The following documents shall be deemed to form and be read and construed as part of this Agreement, viz.:

   a) GeM Bid Document No. …… dated ……..;
   b) GeM Sanction No……. dated ……..;
   c) GeM Contract No…….. dated ……
   d) The Bid Form and the Price Schedule submitted by the Bidder;
   e) The Schedule of Requirements;
   f) The Functional &Technical Specifications;
   g) The Conditions of Contract;
   h) The Purchaser's Notification of Award/Purchase Order.
   i) The RFP including Addendum/s & corrigendum/s.

3. In consideration of the payments to be made by the Purchaser to the Supplier as hereinafter mentioned, the Supplier hereby covenants with the Purchaser to provide the goods and services and to remedy defects therein in conformity in all respects with the provisions of the Contract.

4. The Purchaser hereby covenants to pay the Supplier in consideration of the provision of the goods and services and the remedying of defects therein, the Contract Price or such other sum as may become payable under the provisions of the Contract at the times and in the manner prescribed by the Contract.

Brief particulars of the goods and services which shall be supplied/provided by the Supplier are as under:

Sl. No.	**Brief description of goods & services**	**Quantity to be supplied**	**Unit price**	**Total price (including taxes)**

TOTAL VALUE (including taxes):

DELIVERY SCHEDULE:

IN WITNESS whereof the parties hereto have caused this Agreement to be executed in accordance with their respective laws the day and year first above written.

Signed, Sealed and Delivered by the

said ..... (For Indian Bank)

in the presence of: .....

Signed, Sealed and Delivered by the

said ..... (For the supplier)

in the presence of:.....

GeM Bid Ref: GEM/2025/B/6707442 **Date:** ***20.09.2025***

ANNEXURE-IV

Performance Security Format

Bank Guarantee No. Date:

To:
The Asst. General Manager
Indian Bank
Information System Security Department
Ground Floor
66, Rajaji Salai,
Chennai – 600 001

WHEREAS ..... (Name of Supplier) hereinafter called "the Supplier") has undertaken, in pursuance of Contract No..... dated ..... to.....(Description of Goods and Services) (hereinafter called "the Contract").

AND WHEREAS it has been stipulated by you in the said Contract that the Supplier shall furnish you with a Bank Guarantee by a recognized bank for the sum specified therein as security for compliance with the Supplier's performance obligations in accordance with the RFP & Contract including Maintenance and Repairs of the entire system including cost of spares during warranty period.

AND WHEREAS we have agreed to issue a Guarantee in your favour on the request of the Supplier:

THEREFORE, WE hereby affirm that we are Guarantors and responsible to you, on behalf of the Supplier, up to a total sum of Rs..... ..... (Amount of the Guarantee in Words and Figures) and we undertake to pay you, upon your first written demand declaring the Supplier to be in default under the Contract and without any demur, cavil or protest, any sum or sums within the limit of ..... (Amount of Guarantee) as aforesaid, without your needing to prove or to show grounds or reasons for your demand or the sum specified therein.

This guarantee is valid until the .....day of.....20--

Signature of Authorized Official with Seal

.....

Date.....2025

Address: .....

GeM Bid Ref: GEM/2025/B/6707442 **Date:** ***20.09.2025***

.....

NOTE:

1. Supplier should ensure that seal and code no of the signatory is put by the bankers, before submission of the bank guarantee.
2. Bank Guarantee issued by a scheduled commercial Banks located in India and shall be on a Non-Judicial Stamp Paper of requisite value.

GeM Bid Ref: GEM/2025/B/6707442 **Date:** ***20.09.2025***

ANNEXURE-V

Pre-Contract Integrity Pact

(To be submitted on Non - Judicial Stamp Paper)

PRE-CONTRACT INTEGRITY PACT

Between

Indian Bank hereinafter referred to as "The Bank''

and

……. hereinafter referred to as "The Bidder/Contractor"

Preamble

The Bank intends to award, under laid down organizational procedures, contract/s for Incident Response (IR), Cyber/Digital forensic services, Red Team, Tabletop & Cyber Drill Exercise services. The Bank values full compliance with all relevant laws of the land, rules, regulations, economic use of resources and of fairness / transparency in its relations with its Bidder(s) and / or Contractor(s).

In order to achieve these goals, the Bank will appoint an Independent External Monitor/s (IEM), who will monitor the tender process and the execution of the contract for compliance with the principles mentioned above.

Section 1 – Commitments of the Bank

1. The Bank commits itself to take all measures necessary to prevent corruption and to observe the following principles:

a) No employee of the Bank, personally or through family members, will in connection with the tender for, or the execution of a contract, demand, take a promise for or accept, for self or third person, any material or immaterial benefit which the person is not legally entitled to.

b) The Bank will, during the tender process treat all Bidder(s) with equity and reason. The Bank will in particular, before and during the tender process, provide to all Bidder(s) the same information and will not provide to any Bidder(s) confidential/additional information through which the Bidder(s) could obtain an advantage in relation to the tender process or the contract execution.

c) The Bank will exclude from the process all known prejudiced persons.

2. If the Bank obtains information on the conduct of any of its employees which is a criminal offence under the IPC/PC Act, or if there be a substantive suspicion in this regard, the Bank will inform the Chief Vigilance Officer(CVO) and in addition can initiate disciplinary actions.

GeM Bid Ref: GEM/2025/B/6707442 **Date:** ***20.09.2025***

Section 2 – Commitment of the Bidder(s)/ Contractor(s)

1. The Bidder(s) / Contractor(s) commit themselves to take all measures necessary to prevent corruption. He commits himself to observe the following principles during his participation in the tender process and during the contract execution.

a. The Bidder(s) / Contractor(s) will not, directly or through any other person or firm, offer, promise or give to any of the Bank's employees involved in the tender process or the execution of the contract or to any third person any material or other benefit which he/she is not legally entitled to, in order to obtain in exchange any advantage of any kind whatsoever during the tender process or during the execution of the contract.

b. The Bidder(s) / Contractor(s) will not enter with other Bidders into any undisclosed agreement or understanding, whether formal or informal. This applies in particular to prices, specifications, certifications, subsidiary contracts, submission or non-submission of bids or any other actions to restrict competitiveness or to introduce cartelization in the bidding process.

c. The Bidder(s) / Contractor(s) will not commit any offence under the relevant IPC/PC Act: further, the Bidder (s) / Contractor (s) will not use improperly, for purpose of competition or personal gain, or pass on to others, any information or documents provided by the Bank as part of the business relationship, regarding plans, technical proposals and business details, including information contained or transmitted electronically.0

d. The Bidder (s) / Contractor (s) of foreign origin shall disclose the name and address of the Agents/Representatives in India, if any. Similarly, the Bidder(s)/Contractor (s) of Indian Nationality shall furnish the name and address of the foreign principals, if any. Further, as mentioned in the "Guidelines on Indian Agents of Foreign Suppliers'' shall be disclosed by the Bidder (s) / Contractor (s). Further as mentioned in the Guidelines, all the payments made to the Indian Agent/Representative have to be in Indian Rupees only. Copy of the ''Guidelines on Indian Agents of Foreign Suppliers'' is placed at Annexure.

e. The Bidder (s) / Contractor (s) will, when presenting his bid, disclose any and all payments he has made, is committed to or intends to make to agents, brokers or any other intermediaries in connection with the award of the contract.

2. The Bidder (s) / Contractor (s) will not instigate third persons to commit offences outlined above or be an accessory to such offences.

Section 3– Disqualification from tender process and exclusion from future contracts

If the Bidder(s) / Contractor(s), before award or during execution has committed a transgression through a violation of Section 2, above or any other form such as to put his reliability or creditability in question, the Bank is entitled to disqualify the Bidder(s) / Contractor(s) from the tender process.

Section 4 – Compensation for Damages

1. If the Bank has disqualified the Bidder(s) from the tender process prior to the award according to Section 3, the Bank is entitled to demand and recover the damages equivalent to Bid Security and this bid security will be forfeited.

2. If the Bank has terminated the contract according to Section 3, or if the Bank is entitled to terminate the contract according to Section 3, the Bank shall be entitled to demand and recover from the Contractor the liquidated damages equivalent to the amount of the contract value.

Section 5 – Previous Transgression

1. The Bidders declares that no previous transgressions occurred in the last three years with any other Company in any country conforming to the anti-corruption approach or with any other Public Sector Enterprises in India that could justify his exclusion from the tender process.
2. The Bidder agrees that if he makes incorrect statement on this subject, bidder is liable to be disqualified from the tender process or the contract, if already awarded, is liable to be terminated for such reason.
3. The imposition and duration of the execution of the bidder will be determined by the bidder based on the severity of transgression.
4. The Bidder/Contractor acknowledges and undertakes to respect and uphold the Bank absolute right to resort to and impose such exclusion.
5. Apart from the above, the Bank may take action for banning of business dealings/holiday listing of the Bidder/ Contractor as deemed fit by the Bank.
6. If the Bidder/Contractor can prove that he has resorted/recouped the damage caused by him and has implemented a suitable corruption prevention system, the Bank may, at its own discretion, as per laid down organizational procedures, revoke the exclusion prematurely.

Section 6 – **Equal treatment of all Bidders/ Contractors/ Sub-Contractors**

1. The Bidder(s)/Contractor(s) undertake(s) to demand from all sub-contractors a commitment in conformity with this Pre-Contract Integrity Pact, and to submit it to the Bank before contract signing. The Bidder(s)/Contractor(s) shall be responsible for any violation(s) of the principles laid down in this agreement/Pact by any of its Sub-contractors/Sub-vendors.
2. The Bank will enter into agreement with identical conditions as this one with all Bidders/Contractors.
3. The Bank will disqualify from the tender process all bidders who do not sign this Pact or violate its provisions.

Section 7 – **Criminal charges against violating Bidder(s) /Contractor(s) /Sub contractor(s)**

If the Bank obtains knowledge of conduct of a Bidder, Contractor or Sub-contractor or of an employee or a representative or an associate of a Bidder, Contractor or Subcontractor which constitutes corruption, or of the Bank has substantive suspicion in this regard, the Bank will inform the same to the Chief Vigilance Officer.

Section 8 – Independent External Monitor / Monitors

1. The Bank appoints competent and credible Independent External Monitor for this Pact. The task of the Monitor is to review independently and objectively, whether and to what extent the parties comply with the obligations under this agreement.
2. The Monitor is not subject to instructions by the representatives of the parties and performs his functions neutrally and independently. It will be obligatory for him to treat the information and documents of the Bidders/Contractors as confidential. He reports to the Authority designated by the Bank.
3. The Bidder(s)/Contractor(s) accept that the Monitor has the right to access without restriction to all Project documentations of the Bank including that provided by the Contractor. The Contractor will also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The same is applicable to Subcontractors. The Monitor is under contractual obligation to treat the information and documents of the Bidders)/Contractors(s)/Subcontractors(s) with confidentiality.
4. The Bank will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between the Bank and the Contractor. The parties offer to the Monitor the option to participate in such meetings.
5. As soon as the Monitor notices, or believes to notice, a violation of this agreement, he will so inform the Management of the Bank and request the Management to discontinue or take corrective action, or to take other relevant action. The Monitor can in this regard submit non-binding recommendations. Beyond this, the Monitor has no right to demand from the parties that they act in a specific manner, refrain from action or tolerate action.
6. The Monitor will submit a written report to the Authority designated by the Bank, within 8 to 10 weeks from the date of reference or intimation to him by the Bank and, should the occasion arise submit proposals for correcting problematic situations.
7. If the Monitor has reported to Authority designated by the Bank, a substantiated suspicion of an offence under relevant IPC/PC Act, and the Authority designated by the Bank has not, within the reasonable time taken visible action to proceed against such offence or reported it to the Chief Vigilance Officer, the Monitor may also transmit this information directly to the Central Vigilance Commissioner.
8. The word **'Monitor'** would include both singular and plural.

Section 9 – **Pact Duration**

This pact begins when both parties have legally signed it. It expires for the Contractor 12 months after the last payment under the contract, and for all other Bidders 6 months after the contract has been awarded on whomsoever it may be.

If any claim is made/lodged during this time, the same shall be binding and continue to be valid despite the lapse of this pact as specified above, unless it is discharged/determined by the Bank.

Section 10 – Examination of Books of Accounts

In case of any allegation of, violation of any provisions of this Pre-Contract Integrity Pact or payment of commission, the Bank or its agencies shall be entitled to examine the Books of Accounts of the Bidder and the Bidder shall provide necessary information of the relevant financial documents in English and shall extend all possible help for the purpose of such examination.

Section 11 – Other provisions

1. This agreement is subject to Indian Law, Place of performance and jurisdiction is the Corporate Office of the Bank, i.e. Chennai.
2. Changes and supplements as well as termination notices need to be made in writing. Side agreements have not been made.
3. If the Contractor is a partnership or a Consortium, this agreement must be signed by all partners or Consortium members. In case of a Company, the Pact must be signed by a representative duly authorized by Board resolution.
4. Should one or several provisions of this agreement turn out to be invalid, the reminder of this agreement remains valid. In this case, the parties will strive to come to an agreement to their original intentions.
5. In the event of any contradiction between the Pre-Contract Integrity Pact and its Annexure, the Clause in the Pre-Contract Integrity Pact will prevail.
6. Parties signing this Pact shall not approach the courts while representing the matters to Independent External Monitors and he/she will await their decision in the matter.
7. Any dispute or difference arising between the parties with regard to the terms of this Agreement/Pact, any action taken by the Bank in accordance with this Agreement/Pact or interpretation thereof shall not be subject to arbitration.

The parties hereby sign this Pre-Contract Integrity Pact at ……on ……

GeM Bid Ref: GEM/2025/B/6707442 **Date:** ***20.09.2025***

(For & On behalf of the Bank)	(For & On behalf of Bidder/Contractor)
(Office Seal)	(Office Seal)
Place _____	Place _____
Date _____	Date _____
Witness 1:	Witness 1:
(Name & Address) _____	(Name & Address) _____
_____	
_____	
_____	
_____	
_____	
Witness 2:	Witness 2:
(Name & Address) _____	(Name & Address) _____
_____	
_____	
_____	
_____	

GeM Bid Ref: GEM/2025/B/6707442 **Date:** ***20.09.2025***

ANNEXURE-VI

Non-Disclosure Agreement

THIS AGREEMENT made and entered into at ……on this the ……day of……202… between **INDIAN BANK**, a body corporate constituted under the Banking Companies (Acquisition & Transfer of Undertakings) Act 1970, having Head Office, Information System Security Department, 66 Rajaji Salai, Chennai - 600001, hereinafter called the "**BANK**" which term shall wherever the context so require includes its successors and assigns

AND

M/s……. Limited a company registered under the Companies Act having its registered office at…… hereinafter called the "Supplier" which term shall wherever the context so require includes its successors and assigns, **WITNESSETH**:

WHEREAS

The Bank is inter-alia engaged in the business of banking and intends to procure Incident Response (IR), Cyber/Digital forensic services, Red Team, Tabletop & Cyber Drill Exercise Services.

M/s……. Limited has been engaged in the business of providing Incident Response (IR), Cyber/Digital forensic services, Red Team, Tabletop & Cyber Drill Exercise Services.

The parties have entered into agreement dated _____ for providing Incident Response (IR), Cyber/Digital forensic services, Red Team, Tabletop & & Cyber Drill Exercise Services (herein after referred to as "purpose")" and have established business relationship between themselves. In course of the said purpose, it is anticipated that each party may disclose or deliver to the other certain or some of its trade secrets or confidential or proprietary information. The parties have agreed that disclosure and use of such confidential information shall be made and on the terms and conditions of this agreement.

NOW THERFORE THIS AGREEMENT WITNESSETH and it is hereby agreed by and between the parties hereto as follows:

1. Confidential information

Confidential Information means all information disclosed/ furnished by either party to another party in connection with the Purpose. Confidential Information shall include customer data, any copy, abstract, extract, sample, note or module thereof and all electronic material or records, tenders and other written, printed or tangible thereof and include all information or material that has or could have commercial value or other utility in the business in which disclosing party is engaged.

Receiving party may use the information solely for and in connection with the Purpose.

2. Use of Confidential Information

Each party agrees not to use the other's confidential information for any purpose other than for the specific purpose. Any other use of such confidential information by any party shall be made only upon the prior written consent from the authorized representative of the other party or pursuant to subsequent agreement between the Parties hereto.

The receiving party shall not commercially use or disclose for commercial purpose any confidential information or any materials derived there from, to any other person or entity other than persons in the direct employment of the Receiving Party who have a need to access to and knowledge of the confidential information solely for the purpose authorized above. Whenever, it is expedient under the contract, the Receiving Party may disclose confidential information to consultants/third party only if the consultant/ third party has executed non-disclosure agreement with the Receiving Party that contains terms and conditions that are no less restrictive than these and such consultant should also be liable to the original disclosing party for any unauthorized use or disclosure. The Receiving party shall take appropriate measures by instruction and written agreement prior to disclosure to such employees to assure against unauthorized use or disclosure. The Receiving Party agrees to notify the Disclosing Party immediately if it learns of any use or disclosure of the Disclosing party's confidential information in violation of the terms of this Agreement.

Neither party shall make news release, public announcements, give interviews, issue or publish advertisements or Agreement, the contents/provisions thereof, other information relating to this agreement, the purpose, the Confidential information or other matter of this agreement, without the prior written approval of the other party.

Upon written request by the Bank, the Supplier shall:

(i) cease using the Confidential information,

(ii) return the Confidential Information and all copies, notes or extracts thereof to the Bank within seven (7) business days of receipt of request and

(iii) confirm in writing that the Receiving Party has complied with the obligations set forth in this paragraph."

3. Exemptions

The obligations imposed upon either party herein shall not apply to information, technical data or know how whether or not designated as confidential, that:

Is already known to the Receiving party at the time of the disclosure without an obligation of confidentiality

Is or becomes publicly known through no unauthorized act of the Receiving party

Is rightfully received from a third party without restriction and without breach of this agreement

Is independently developed by the Receiving party without use of the other party's confidential information and is so documented.

Is disclosed without similar restrictions to a third party by the Party owning the confidential information

Is approved for release by written authorization of the disclosing party; or

Is required to be disclosed pursuant to any applicable laws or regulations or any order of a court or a governmental body; provided, however that the Receiving party shall first have given notice to the Disclosing Party and made a reasonable effort to obtain a protective order requiring that the confidential information and / or documents so disclosed used only for the purposes for which the order was issued.

4. Term

This agreement shall be effective from the date of the execution of this agreement and shall continue till expiration or termination of this agreement due to cessation of the business relationship between the parties. Upon expiration or termination as contemplated herein the Receiving party shall immediately cease any or all disclosures or uses of confidential information and at the request of the disclosing party, the receiving party shall promptly return or destroy all written, graphic or other tangible forms of the confidential information and all copies, abstracts, extracts, samples, note or modules thereof.

Notwithstanding the above, the obligations of the receiving party in respect of disclosure and confidentiality shall continue to be binding and applicable without limit until such information enters the public domain.

5. Title and Proprietary rights

Notwithstanding the disclosure of any confidential information by the disclosing party to the receiving party, the disclosing party shall retain title and all intellectual property and proprietary rights in the confidential information. No License under any trademark, patent or copyright or application for same which are or thereafter may be obtained by such party is either granted or implied by the conveying of confidential information.

6. Return of confidential information

Upon written demand of the disclosing party, the receiving party shall (I) cease using the confidential information (ii) return the confidential information and all copies, abstracts, extracts, samples, note or modules thereof to the disclosing party within seven (7) days after receipt of notice and (iii) upon request of the disclosing party, certify in writing that the receiving party has complied with the obligations set forth in this paragraph.

7. Remedies

The receiving party acknowledges that if the receiving party fails to comply with any of its obligations hereunder, the disclosing party may suffer immediate, irreparable harm for which monetary damages may not be adequate. The receiving party agrees that, in addition

to all other remedies provided at law or in equity, the disclosing party shall be entitled to injunctive relief hereunder.

8. Entire agreement

This agreement constitutes the entire agreement between the parties relating to the matter discussed herein and supersedes any and all prior oral discussion and/or written correspondence or agreements between the parties. This agreement may be amended or modified only with the mutual written consent of the parties. Neither this agreement nor any rights, benefits and obligations granted hereunder shall be assignable or otherwise transferable.

9. Severability

If any provision herein becomes invalid, illegal or unenforceable under any law, the validity, legality and enforceability of the remaining provisions and this agreement shall not be affected or impaired.

10. Dispute resolution mechanism

In the event of any controversy or dispute regarding the interpretation of any part of this agreement or any matter connected with, arising out of, or incidental to the arrangement incorporated in this agreement, the matter shall be referred to arbitration and the award passed in such arbitration shall be binding on the parties. The arbitral proceeding shall be governed by the provisions of Arbitration and Reconciliation Act 1996 and the place of arbitration shall be Chennai.
Submitting to arbitration may be considered as an additional remedy and it does not preclude the parties to seek redressal/ other legal recourse.

11. Jurisdiction

Any disputearising out of this order will be under the jurisdiction of Courts of Law in Chennai.

12. Indemnity clause

“The receiving party should indemnify and keep indemnified, saved, defended, harmless against any loss, damage, costs etc. incurred and / or suffered by the disclosing party arising out of breach of confidentiality obligations under this agreement by the receiving party etc., officers, employees, agents or consultants.”

13. Governing laws

The provisions of this agreement shall be governed by the laws of India.
In witness whereof, the parties hereto have set their hands through their authorised signatories

Signed, Sealed and Delivered by the

said ..... (For Indian Bank)

in the presence of: .....

Signed, Sealed and Delivered by the

said ..... (For the supplier)

in the presence of: .....

GeM Bid Ref: GEM/2025/B/6707442 **Date:** ***20.09.2025***

ANNEXURE-VII

Declaration For MSE Benefits

(*To be submitted on the letter head of the bidder signed by* Director/Company Secretary)

To,
The Asst. General Manager
Indian Bank
Information System Security Department
Ground Floor
66, Rajaji Salai,
Chennai – 600 001

Dear Sirs,

Sub: Request for Proposal for Selection and Appointment of service provider for Incident Response (IR), Cyber/Digital forensic services, Red Team, Tabletop & Cyber Drill Exercise.

Ref: Your RFP No. GEM/2025/B/6707442 dated 20.09.2025

Dear Sir,

This has reference to our bid submitted in response to your Request for Proposal (RFP) Ref. No. RFP No. GEM/2025/B/6707442 dated 20.09.2025 floated for Selection and Appointment of service provider for Incident Response (IR), Cyber/Digital forensic services, Red Team, Tabletop & Cyber Drill Exercise. We have carefully gone through the contents of the above referred RFP and hereby undertake and confirm that, as per the Govt. Of India guidelines, we are eligible to avail the following MSE benefits in response to your RFP floated, as referred above.

a) Exemption on submission of bid security

In case, at any later stage, it is found or established that, the above undertaking is not true then the Bank may take any suitable actions against us viz. Legal action, Cancelation of Notification of Award/contract (if issued any), Blacklisting & debarment from future tender/s etc.

Yours Sincerely

For M/s _____

Signature
Name:
Designation: Director/Company Secretary
Place:
Date:
Seal & Stamp

GeM Bid Ref: GEM/2025/B/6707442 **Date:** ***20.09.2025***

ANNEXURE-VIII

Declaration On Procurement From a Bidder of a Country which shares a land border with India

(THE BIDDER SHOULD GIVE THE FOLLOWING UNDERTAKING / CERTIFICATE ON ITS LETTERHEAD)

To, Date

The Asst. General Manager
Indian Bank
Information System Security Department
Ground Floor
66, Rajaji Salai,
Chennai – 600 001

Dear Sirs,

Sub: Request for Proposal for Selection and Appointment of service provider for Incident Response (IR), Cyber/Digital forensic services, Red Team, Tabletop & Cyber Drill Exercise.

Ref: Your RFP No. GEM/2025/B/6707442 dated 20.09.2025

I have read the clause regarding restriction on procurement from a bidder of a country which shares a land border with India; I certify that **<< name of the firm>>** is not from such a country or, if from such a country, has been registered with the Competent Authority. I hereby certify that we fulfils all requirements in this regard and is eligible to be considered. [Evidence of valid registration by the Competent Authority shall be attached, wherever applicable.]

Signature of Authorized Official

Name and Designation with Office Seal

Place:

Date:

GeM Bid Ref: GEM/2025/B/6707442 **Date:** ***20.09.2025***

ANNEXURE-IX

Certificate of Local Content as per Make in India Guidelines

To, Date

The Asst. General Manager
Indian Bank
Information System Security Department
Ground Floor
66, Rajaji Salai,
Chennai – 600 001

Dear Sirs,

Sub: Request for Proposal for Selection and Appointment of service provider for Incident Response (IR), Cyber/Digital forensic services, Red Team, Tabletop & Cyber Drill Exercise.

Ref: Your RFP No. GEM/2025/B/6707442 dated 20.09.2025

This is to certify that proposed _____ **<product details>** is having the local content of_____ % as defined in the above mentioned RFP.

The details of location(s) at which the local value addition is made are as under

S.No.	Make and Model / Details of services	Name of Place

Bidder shall submit the above details in respect of the goods proposed to be supplied/ solutions proposed to be deployed for providing the testing services.

This certificate is submitted in reference to the Government of India, Ministry of Commerce and Industry, Department of Industrial Policy and Promotion order number P-45021/ 2/2017-B.E.-II dated 15th June 2017 for the Public Procurement (Preference to Make in India), Order 2017, revision order no. P-45021/ 2/2017-PP (B.E.-II) dated 28th May 2018, revision order no. P-45021/ 2/2017-PP (B.E.-II) dated 29th May 2019 and subsequent revision order no DPIIT Order No. P-45021/2/2017-PP(BE-II) dated June 04, 2020 and subsequent revision order no. P-45021/2/2017-PP (B.E.-II) dated 16th Sept 2020 and subsequent revision Order No. P-45021/2/2017-PP (BE-ll)-Part(4) Vol. II dated 19/07/2024 & its clarifications/amendment (if any)referred to hereinabove.

For Bidder

Signature of authorised signatory
Name and Designation:
Seal:
Date:

For OEM

Signature of authorised signatory
Name and Designation:
Seal:
Date:

GeM Bid Ref: GEM/2025/B/6707442 **Date:** ***20.09.2025***

ANNEXURE-X

Undertaking for Labour Law Compliance

To, Date:

The Asst. General Manager
Indian Bank
Information System Security Department
Ground Floor
66, Rajaji Salai,
Chennai – 600 001

Dear Sirs,

Sub: Request for Proposal for Selection and Appointment of service provider for Incident Response (IR), Cyber/Digital forensic services, Red Team, Tabletop & Cyber Drill Exercise.

Ref: Your RFP No. GEM/2025/B/6707442 dated 20.09.2025

We, M/s_____ undertake that we are solely liable and responsible for compliance of applicable Labour Laws and other rules regulations and ordinances applicable in respect of our employee, agents, representatives and sub-contractors (if allowed) and in particular laws relating to terminal benefits such as pension, gratuity, provident fund, bonus or other benefits to which they may be entitled and the laws relating to contract labour, minimum wages, etc., and the Bank shall have no liability in this regard. We also agree and undertake that during the entire period of RFP process and also during the entire period of the contract/SLA we will not employ or engage any personnel / individual below the Minimum Wages fixed by appropriate Government on this behalf from time to time, as per the provisions of Minimum Wages Act 1948 and other laws as applicable.

Signature of Authorized Official

Name and Designation with Office Seal

Place:

Date:

GeM Bid Ref: GEM/2025/B/6707442 **Date:** ***20.09.2025***

ANNEXURE-XI

Pre-Bid Query Format

(to be provided in MS-Excel format)

Sub: Request for Proposal for Selection and Appointment of service provider for Incident Response (IR), Cyber/Digital forensic services, Red Team, Tabletop & Cyber Drill Exercise.

Ref: RFP No. GEM/2025/B/6707442 dated 20.09.2025

Bidder's Name:

S.No	Page No	Para No.	Description	Query details

Signature of Authorized Signatory

Name:

Designation:

Seal:

Date:

GeM Bid Ref: GEM/2025/B/6707442 **Date:** ***20.09.2025***

ANNEXURE-XII

Experience Details of the Bidder/OEM

Ref: RFP No. GEM/2025/B/6707442 dated 20.09.2025

(Submit photocopies of Purchase Orders as supporting documents for each item as per eligibility & evaluation criteria separately)

S.No.	Name of Organization for whom services rendered	Nature of Work	Project Details		
			Period (No. of Months)	Start Date	Date of Completion of Services
1.					
2.					
3.					

The Incident Response & Cyber/Digital Forensics Services being maintained by our organization, M/s _____, to the afore mentioned organizations having at least 250 branches/offices across India. The services are satisfactory, and client references have been submitted separately for each organization, as detailed in Annexure-XVII.

Signature of Authorized Signatory

Name:

Designation:

Seal:

Date:

Note- The above details should preferably be provided by the bidder/OEM on their (organization) letter head.

GeM Bid Ref: GEM/2025/B/6707442 **Date:** ***20.09.2025***

ANNEXURE-XIII

Turnover, Net Worth and P&L Details

(Bidders have to submit photocopies of Audited Balance Sheet / P&L)

Ref: RFP No. GEM/2025/B/6707442 dated 20.09.2025

(Amount in Rs.)

F Y	*Turnover*	*Net Profit and Loss*	*Net worth*
2021-22			
2022-23			
2023-24			
2024-25			

Signature of Authorized Signatory

Name:

Designation:

Seal:

Date:

GeM Bid Ref: GEM/2025/B/6707442 **Date:** ***20.09.2025***

ANNEXURE-XIV

BID SECURITY FORM

To,
The Asst. General Manager
Indian Bank
IT Department,3rd Floor
66, Rajaji Salai,
Chennai – 600 001

Sub: Request for Proposal for Selection and Appointment of service provider for Incident Response (IR), Cyber/Digital forensic services, Red Team, Tabletop & Cyber Drill Exercise.

GeM Bid Ref: **GEM/2025/B/6707442 dated 20.09.2025**

Whereas..... *(Hereinafter called "the Bidder")* who intends to submit its bid..... for the supply of ..... *(name and/or description of the goods)* (Hereinafter called "the Bid") in terms of RFP Ref……..dated……...

In compliance with the terms of said RFP, the Bidder is required to provide Bid Security of Rs…….. which may also be provided in the form of Bank Guarantee from a

KNOW ALL PEOPLE by these presents that We..... *(name of bank)* of ..... (name of country), having our registered office at ..... *(address of bank)* (hereinafter called "the Bank" which term shall include its successors and permitted assigns), are bound unto Indian Bank (hereinafter referred as " the Purchaser" which term shall include its successors and permitted assigns) in the sum of Rs. _____for which payment well and truly to be made to the Purchaser, the Bank guarantees said payment and binds itself, its successors, and assigns by these presents. Sealed with the seal of the Bank this ____ day of _____.

THE CONDITIONS of this obligation are:

1. If the Bidder
   (a) withdraws its Bid during the period of bid validity specified by the Bidder on the Bid Form; or
   (b) does not accept the correction of errors in accordance with the terms of RFP; or
2. If the Bidder, having been notified of the acceptance of its bid by the Bank during the period of bid validity:
   (a) fails or refuses to execute the Contract Form, if required; or
   (b) fails or refuses to furnish the performance security, in accordance with the terms of RFP.

We undertake to pay to the Purchaser up to the above amount upon receipt of its first written demand without any demur, cavil or protest and without the Purchaser having to substantiate its demand, provided that in its demand the Purchaser will note that the amount claimed by it is due to it, owing to the occurrence of one or more of the conditions, specifying the occurred condition or conditions.

GeM Bid Ref: GEM/2025/B/6707442 **Date:** ***20.09.2025***

This guarantee will remain in force up to and including forty-five (45) days after the period of the bid validity i.e. upto…… and any demand in respect thereof should reach the Bank not later than the above date.

(Seal & Signature of the Bank official)

NOTE: 1. Bidder should ensure that the seal and CODE No. of the signatory is put by the bankers, before submission of the bank guarantee.
2. Bank Guarantee to be issued by banks located in India and shall be on a Non-Judicial Stamp Paper of requisite value

GeM Bid Ref: GEM/2025/B/6707442 **Date:** ***20.09.2025***

Annexure-XV
MANUFACTURERS' AUTHORIZATION FORM

(Letter to be submitted by the OEM on its official letter head)

Ref. No. Dated

To
The Asst. General Manager
Indian Bank
Information System Security Department,
Ground Floor
66, Rajaji Salai,
Chennai – 600 001

Sub: Request for Proposal for Selection and Appointment of service provider for Incident Response (IR), Cyber/Digital forensic services, Red Team, Tabletop & Cyber Drill Exercise.

GeM Bid Ref: **GEM/2025/B/6707442 dated 20.09.2025**

Dear Sir,

We _____ who are established and reputable manufacturers/Service Providers of _____ *(name & descriptions of goods/services offered)* having factories/Offices at (*address of factory/Office)* do hereby authorize M/s _____ *(Name and address of Bidder)* to submit a Quote, and sign the contract with you for the goods manufactured by us against the above RFP (Request for Proposal).

We hereby extend our full warranty as per Conditions of Contract for the goods and services offered for supply by the above firm against this RFP (Request for Proposal). We duly authorize the said firm to act on our behalf in fulfilling all installation, technical support and Annual maintenance obligations required by the Contract.

Yours faithfully,

(Name)
(Name of Manufacturer)

Note: This letter of authority should be on the letterhead of the manufacturer and should be signed by a person competent and having the power of attorney to bind the manufacturer.

GeM Bid Ref: GEM/2025/B/6707442 **Date:** ***20.09.2025***

Annexure-XVI
Undertaking of Authenticity
(To be submitted on the letter head from the OEM of the proposed product)

To
The Asst. General Manager
Indian Bank
IT Department, 3rd Floor
66, Rajaji Salai,
Chennai – 600 001

Dear Sir,

Sub: Request for Proposal for Selection and Appointment of service provider for Incident Response (IR), Cyber/Digital forensic services, Red Team, Tabletop & Cyber Drill Exercise.

GeM Bid Ref: **GEM/2025/B/6707442 dated 20.09.2025**

With reference to the Product being quoted to you by our authorized service partner …….. against your above mentioned RFP, we hereby undertake that all the components /parts /assembly / software etc. used in the Product to be supplied will be original new components / parts / assembly / software only, from respective Original Equipment Manufacturers (OEMs) of the Products only and that no refurbished / duplicate / second hand components /parts/ assembly / software shall be supplied or shall be used or no malicious code are built-in in the Product being supplied.

We also undertake that in respect of licensed operating systems and other software utilities to be supplied, the same will be sourced from authorized sources and supplied with Authorized License Certificate (i.e., Product keys on Certification of Authenticity in case of Microsoft Windows Operating System).

In case of default and/or the Bank finds that the above conditions are not complied with, we agree to take back the Product(s) supplied and return the money paid by you, in full within seven days of intimation of the same by the Bank, without demur or any reference to a third party and without prejudice to any remedies the Bank may deem fit.

We also take full responsibility for both Product(s) & Service(s) as per the content of the RFP even if there is any defect by our authorized Service Centre / Reseller / SI etc.

Signature of Authorized Signatory

Name:
Designation:
Seal:
Date:

GeM Bid Ref: GEM/2025/B/6707442 **Date:** ***20.09.2025***

Annexure-XVII

Client References

Ref: RFP No. GEM/2025/B/6707442 dated 20.09.2025

Name of the Organization:
<<Office Address>>
Official Phone Number:

Bidder/OEM M/s _____ has successfully supplied, deployed and are maintaining the Incident Response & Cyber/Digital Forensic Services, as outlined below. The services provided by M/s _____ (Bidder Name) is/was satisfactory.

S.No.	Nature of Work	Project Details		
		Period (No. of Months)	Start Date	Date of Completion of Services
1.				

Our organization has more than 250 branches/offices in India.

Signature of Authorized Signatory

Name:

Designation:

Seal:

Date:

Note- The above details should preferably be provided by the client on their (organization) letter head.

GeM Bid Ref: GEM/2025/B/6707442 **Date:** ***20.09.2025***

Annexure-XVIII

Software Bill of Materials (SBOM)

(Bidders are required to submit the details of the software components in accordance with the Software Bill of Materials (SBOM) provided below)

Ref: RFP No. GEM/2025/B/6707442 dated 20.09.2025

Component Name	Name of the software component or library
Component Version	Version number or identifier
Component Description	Brief description or summary
Component Supplier	Vendor, third-party supplier, or open-source project.
Component License	License under which the software component is distributed, including details such as the license type, terms, and restrictions.
Component Origin	Source or origin of the software component (i.e, proprietary, open-source, or obtained from a third-party vendor)
Component Dependencies	Any other software components or libraries that the current component depends on, including their names and versions.
Vulnerabilities	Information about known security vulnerabilities or weaknesses associated with the software component, including severity ratings and references to security advisories or CVE identifiers
Patch Status	Patch or update status of the software component
Release Date	Date when the software component was released or made available for use.
End-of-Life (EOL) Date	Date when support or maintenance for the software component is scheduled to end
Criticality	Criticality or importance of the software component to the overall functionality or security of the application, often categorized as critical, high, medium, or low.
Usage Restrictions	Any usage restrictions or limitations associated with the software.

	component, such as export control restrictions or intellectual property rights.
Checksums or Hashes	Cryptographic checksums or hashes of the software component files to ensure integrity and authenticity.
Comments or Notes	Additional comments, notes, or annotations relevant to the software component.
Author of SBOM Data	The name of the entity that creates the SBOM data for this component.
Timestamp	Record of the date and time of the SBOM data assembly.
Executable Property	Attributes indicating whether a component within an SBOM can be executed.
Archive Property	Characteristics denoting if a component within an SBOM is stored as an archive or compressed file.
Structured Property	Descriptors defining the organized format of data within a component listed in an SBOM
Unique Identifier	A unique identifier is a distinct code assigned to each software component, structured as "pkg:supplier/OrganizationName/ComponentName@Version?qualifiers&subpath,"

Signature of Authorized Signatory

Name:

Designation:

Seal:

Date:

ANNEXURE-XIX

CHECKLIST FOR THE RFP

S.No.	List of Documents to be submitted	Supporting Details
1	ANNEXURE-I - Bid Form	Detail as per format.
2	ANNEXURE-II - Self-Declaration – Blacklisting	Detail as per format.
3	ANNEXURE–III - Contract Form	Detail as per format.
4	ANNEXURE-IV - Performance Security Format	Detail as per format.
5	ANNEXURE-V - Pre-Contract Integrity Pact	Detail as per format.
6	ANNEXURE-VI - Non-Disclosure Agreement	Detail as per format.
7	ANNEXURE-VII - Declaration For MSE Benefits	Detail as per format.
8	ANNEXURE-VIII - Declaration On Procurement From a Bidder of a Country which shares a land border with India	Detail as per format.
9	ANNEXURE-IX - Certificate of Local Content as per Make in India Guidelines (*Optional*)	Detail as per format.
10	ANNEXURE-X - Undertaking for Labour Law Compliance	Detail as per format.
11	ANNEXURE-XI - Pre-Bid Query Format	Detail as per format.
12	ANNEXURE-XII - Experience Details of the Bidder/OEM	Detail as per format.
13	ANNEXURE-XIII - Turnover, Net Worth and P&L Details	Detail as per format.
14	ANNEXURE-XIV - BID SECURITY FORM	Detail as per format.
15	Annexure-XV - MANUFACTURERS' AUTHORIZATION FORM	Detail as per format.
16	Annexure-XVI - Undertaking of Authenticity	Detail as per format.
17	Annexure-XVII - Client References (for each organization)	Detail as per format.
18	Annexure-XVIII - Software Bill of Materials (SBOM)	Detail as per format.

19	Certificate of Incorporation	Copy of Certificate of Incorporation issued by Registrar of Companies
20	Memorandum & Articles of Association	Full address of the registered office along with Memorandum & Articles of Association.
21	Audited financial statements/certificate from CA	Copy of audited financial statements/certificate from CA with Net worth details of three financial years. In case audited balance sheet is not available for 2024-25, the company may provide provisional balance sheet duly signed by Charted Accountant.
22	Professional or higher level of partnership with OEMs	Copy of OEM partnership certificate
23	Board Resolution / Power of Attorney authorizing signatory	Copy of Board Resolution / Power of Attorney authorizing signatory Name and designation.
24	Annexure-XX : SERVICE LEVEL AGREEMENT	Detail as per format.

ANNEXURE-XX

SERVICE LEVEL AGREEMENT

THIS Service Level Agreement made the .....day of.....2025 Between Indian Bank, having its Head Office, Information System Security Department, 66 Rajaji Salai, Chennai - 600001 (hereinafter "the Purchaser") which term shall unless repugnant to the context or meaning thereof shall mean its successors and assigns) of the one part and …… (Name of Supplier) having its Registered Office at …… (City and Country of Supplier) (hereinafter called "the Supplier") which term shall unless repugnant to the context or meaning thereof shall mean its successors and permitted assigns) of the other part:

WHEREAS the Purchaser invited bids vide RFP No. ……. for **Selection and Appointment of service provider for Incident Response (IR), Cyber/Digital forensic services, Red Team, Tabletop & Cyber Drill Exercise** (Brief Description of Goods and Services) and has accepted a bid by the Supplier for the provision of those goods and services in the sum for .... (Contract Price in Words and Figures) (hereinafter called "the Contract Price").

NOW THEREFORE THE PARTIES HERETO AGREE AS FOLLOWS:

1) Scope of work

The Bank invites proposals from eligible and experienced service providers for the engagement of the following cybersecurity services, to be delivered on an annual and on demand basis:

1. **Incident Response Readiness Assessment (Annual)** – Evaluation of the Bank's preparedness to detect, respond to, and recover from cyber incidents.
2. **Incident Response Support (On-Demand)** – Expert assistance during the security breach, immediate detection, containment, and remediation to minimize damage and quickly restore normal operations.
3. **Cyber/Digital Forensics Readiness Assessment (Annual)** – Assessment of the Bank's forensic capabilities, tools, and procedures to ensure effective investigation and evidence handling.
4. **Cyber/Digital Forensics Incident Audit / Investigation / Analysis (On-Demand)** – Expert-led forensic analysis and investigation of cyber incidents as and when required.
5. **Red Team Exercises (Annual)** – Simulated adversarial attacks to evaluate the Bank's detection and response capabilities.
6. **Cyber Drills (Annual)** – Scenario-based technical drills to test incident response mechanisms. These may be conducted biannually at the discretion of the Bank.
7. **Tabletop Exercises (Annual)** – Simulated, discussion-based exercises to assess decision-making and coordination during cyber incidents.

Service providers must demonstrate relevant domain expertise, industry certifications, and a proven track record in delivering similar engagements to financial institutions. All services shall be delivered in accordance with applicable regulatory guidelines and industry best practices.

GeM Bid Ref: GEM/2025/B/6707442 **Date:** ***20.09.2025***

Broad Scope of work for Incident Response:

Phase 1:

1. **Incident Response Readiness Assessment (IRRA)**
   This phase will include review of existing monitoring, logging and detection technologies, current network and host architecture, evaluating first response capabilities and Improve Bank's Incident Response Plan and Procedures. Vendor will help the Bank to establish an incident response capability so that Bank is ready to respond to it. Under this preparation phase, which involves preparing for potential cyber incidents by establishing incident response plans, identifying the procedural and technical gaps in existing IT Setup w.r.t. incident response readiness, creating an incident response team having representative from Bank and IR vendor personals, defining their roles and responsibilities, and implementing monitoring and detection systems.

   Workshops/assessment to be conducted with various stakeholders in the Bank by bidder in order to understand Bank environment to enable to Bidders Incident response team to respond, mitigate, recover from attacks as soon as possible. This phase is to review banks existing Incident response plans, technologies deployed, log sources in place to detect/analyses to be checked and reediness in order to respond to attacks/breaches within stipulated timelines. The vendor should perform the gap assessment on existing SOP of Cyber Security incident handling/ Cyber crisis management plan and various other procedure documents.

2. The IRRA should not be only limited to meetings/workshops/trainings, but Infrastructure manipulation capabilities also to be assessed based on various real time use cases, but not limited to:
   VIII. Centralized deployment/execution of IOC scanners or other tools designed to obtain digital evidence.
   IX. Credentials management (e.g. password change policies)
   X. System backup architecture and backup recovery.
   XI. Logging security event sources
   XII. Log sources / security controls check.
   XIII. Assessment of readiness to respond, mitigate, recover from various attack scenarios, but not limited to;
      a. Espionage by threat actors (including state-sponsored groups)
      b. Watering hole attacks
      c. Trusted relationship attacks
      d. Supply chain attacks
      e. Money theft through online banking systems, card processing etc.
      f. ATM jackpotting
      g. Ransomware attacks
      h. Unauthorized access to servers, databases, web applications, network equipment etc.
      i. Insider attacks (leaks, disruption, sabotage, unauthorized access etc.)
      j. Infection using botnets.
      k. Phishing campaigns (links & attachments)
      l. Cryptocurrency mining malware attacks
   XIV. The log sources / security controls should include, but not limited to
      g. DHCP logs
      h. DNS logs

i. Network traffic logs
j. Event logs from endpoints and servers (at the OS level), network & security devices like DLP, EDR, WAF, Firewall, HIPS, VPN, Active Directory etc.
k. Logs of user authorization and activities on business systems
l. Audit logs of user actions on virtual machine servers & cloud platforms.

3. The vendor will help the Bank to prepare incident response team's specific technical methods, strategies, checklists, and forms based on gap assessment.
4. The vendor will provide recommendations on how to improve incident response readiness.
5. The vendor will provide recommendations on how to reconfigure or upgrade existing security event monitoring.
6. The vendor will setup the dedicated IT infrastructure for Indian Bank within India, either physical or in cloud instance (cloud region should be located within India or specific the region of the Incident occurrence), which will be utilized and accessed remotely by IR analysts, during incident response for log analysis and correlation. No logs or metadata should be transferred outside of India. The cloud instances should be preserved at least for 3 years at the end of contract or based on agreed retention period as per Bank written confirmation.
7. During Incident response readiness review exercise the vendor should clearly define below modalities in detail.
   • Incident Response team structure and responsibilities
   • Communication between different teams (IR, ISSD and other stakeholders from Bank) will take place in case of Cyber Incident
   • Procedure of sharing evidence / access to the required logs.
   • The selected vendor will help Bank to prepare and regularly update for the Bank.
8. Establishing required Infrastructure to handle Cyber Incident/ sharing evidence:
   • The successful vendor should establish a process, and deploy/install necessary hardware, software, sensors, scripts, agents for collection of evidence for incident analysis.
   • Assist in clearing/signoff of security review of such tools, devices, and technologies before completion of Phase 1 (IRRA) from bank's side.
9. Recommendations on how to reconfigure or upgrade existing security event monitoring systems, backup solutions, security devices, etc.
10. Provide Incident Response Readiness Assessment Guide.
11. Provide Incident Response Readiness Assessment Report.

Phase 2: Incident Identification

The required manpower and number of days will be utilized in onwards phases, on actual utilization and deployment of IR services.

1. This phase will involve identifying and categorization (e.g., critical, high, medium, low priority) of potential incident in co-ordination with Bank by collecting and analyzing data from various sources, such as intrusion detection systems, log files, applications, devices and network traffic etc.
2. 24*7*365 days dedicated support facility for incident response shall made available by the vendor. The vendor IR staff should be well trained to effectively handle queries

raised by the Bank, whenever a phone call/ email /alert received from Bank's dedicated Officials for probable incident.

3. The Service provider should acknowledge receipt of alert from bank within 2 Hours and start the Incident Response within 4 Hours of reporting of alert from the Bank. Upon confirmed breach, the IR analyst should immediately start working on preliminary information submitted by the Bank. At least 2 IR analyst should be at onsite location (DC, DR, NDR, NDC, HO or CO) of breach, if required, within 24 Hours, excluding travel time.
4. Provide detailed information of the Threat Adversary identified in the initial assessment based on intelligence of service provider and experience.
5. An IR daily status update that covers the days' status summary, action items, intelligence summary, and current recommendations to be provided to bank in writing.
6. Service provider to ensure incident response and forensic investigation report has to be duly vetted by CERT-In empanelled auditor, which should be acceptable to regulators of India.
7. A walkthrough meeting to be conducted on reported findings.

Phase 3: Containment

In this phase, the IR (incident response) team will work to contain the incident to prevent the further damage to affected IT assets and ensure that other IT systems remain unaffected. The bidder shall assist in reporting and notification to Regulatory and statutory authorities, Law Enforcement Agencies, Bank's Public Relations &. Social Media Department, Human Resource Department, News publication etc.

Phase 4: Analysis

This phase will involve analyzing the incident to determine the scope, cause, and extent of the damage. The IR team may further gather and examine evidence, interview witnesses, and use forensic tools to identify the attacker and their methods.

1. Log retention and the logs collected/processed should be available for export in supported formats and not associated without any proprietary formats for audit/compliance purposes.
2. The vendor should be able to perform investigation on different technologies, assets inclusive of all technologies, applications, devices available in Bank's IT-Ecosystem and the various resources required during the investigation should be scalable.

Phase 5: Eradication

The vendor should identify and mitigating all vulnerabilities that were exploited by the Threat Actor. This phase involves removing the threat from affected systems completely to bring to their original state.

Phase 6: Recovery/Monitoring:

In this phase, the incident response team works to restore the attacked system/ operations to normal state and should ensure that the systems are functioning normally and remediate vulnerabilities to prevent similar incidents in the bank. The bidder should perform continuous monitoring of the network/in for the agreed period of time based on the severity of incident in order to make sure that there is no remanence of the threat actor left in the network.

Phase 7: Reporting & Lesson learned:

The successful vendor should provide User awareness training, updating relevant policies and procedures, and reviewing incident response plans and shall also provide;

1. Threat Briefing to Executive Board Members. Assist in reporting and notification to Regulatory and statutory authorities, Law Enforcement Agencies, Bank's Public Relations &. Social Media Department, Human Resource Department, News publication etc.
2. Root cause analysis of the incident for corrective actions to be submitted to Bank for improvements in robustness and resilience in Cyber Security posture of Bank's IT infrastructure.
3. The incident response team should conduct a post incident review to identify what worked well and what could be improved for future incidents and lesson learned. The IR team must give inputs to update Bank's incident response plan and suggest action plan for implementing necessary changes and improvement needed.

Other services to be provided by the Bidder but not limited to:

4. Service provider shall provide the security incident first responder training to key staff members identified by bank to identifying and protecting the scene, preserving evidence, collect data, maintain chain of custody etc.
5. Service provider shall conduct trainings of Bank personnel to ensure proper documentation, procedure, policies during a forensic investigation.
6. Service provider shall understand the legal requirements and implications of forensic investigations including privacy laws and regulations.
7. Service provider shall provide legal evidence which are valid in courts and present the same to the court.
8. Service provider shall develop a forensic response plan mentioning the steps to be taken while collecting & preserving digital evidence after a ransomware attack.
9. Service provider shall determine how critical data is stored and how it can be accessed during forensic investigation.
10. Service provider shall assist regulatory bodies during their forensics investigation, if required.
11. The Incident Response Team/vendor shall be able to use below methodologies for handling of Cyber Incident and response.

1	The Bidder must be able to Conduct host-based sweeping activities.
2	The Bidder must be able to search for malware and tools linked to specific attack groups that are collectively known as Advanced Persistent Threat (APT) groups.
3	The Bidder must be able to utilize a mix of automated and manual techniques to identify indicators of compromise.
4	The Bidder must be able to search for various artifacts not limited to: staging paths, persistence mechanisms, lateral movement mechanisms, registry keys, etc.
5	The Bidder must have to capability to sweep the Endpoint with IOC's related to Custom Malware looking for Persistence Mechanism and Lateral Movement techniques.

6	The Bidder must be able to scan windows end points, servers and virtual environments as a part of the compromise assessment to identify evidence of compromise.
7	The Bidder must have an ability to scan different flavors of Windows, Linux & Unix environments for evidence of compromise.
8	The Bidder must be able to also search for malware and tools associated with on-APT groups.
9	The Bidder must inspect IT systems for IOCs Identifying file names and hashes of known malware and utilities.
10	The Bidder must inspect IT systems for IOCs, Analyzing file import tables of each executable file for specific IOCs
11	The Bidder must inspect IT systems for IOCs Reviewing all running processes and network connections for references to known “hostile” domains.
12	The Bidder must inspect IT systems for IOCs Inspecting registry keys and values associated with known malware, and for persistence mechanisms that could lead to the detection of unknown malware.
13	The Bidder must inspect IT systems for IOCs Identifying specific global mutexes used by processes.
14	The Bidder must inspect IT systems for IOCs Detecting rootkits, hidden files, and hidden processes.
15	The Bidder must be able to analyses Web Shells for evidence collection.
16	The Bidder must be able to analyse event logs generated from different IT systems for evidence collection.
17	The Bidder must be able to automate collection and analysis of evidence and minimize manual activities
18	The Bidder must be able to analyse a majority of assets (at least 85% or higher) and not limit to dipstick analysis on a limited set of assets
19	The Bidder must be able to Conduct network monitoring activities
20	The Bidder must have the capability to sweep the Network with IOC's related to Custom Malware looking for Lateral Movement techniques
21	The Bidder must be able to monitor the Network traffic for Backdoor command and control protocols
22	The Bidder must be able to monitor the Network traffic for Communication to IP addresses that are associated with targeted attacker activity.
23	The Bidder must be able to monitor the Network traffic for Resolution of domain names that associates with targeted attacker activity
24	The Bidder must be able to monitor the Network traffic for Certificates that are used by attackers to encrypt malicious traffic.
25	The Bidder must be able to Conduct log data analysis activities.

26	If required, the bidder must have the ability to perform malware analysis and reverse engineering of malware samples using both automated and manual techniques and provide host-based and network-based indicators that are used to find the malware variants in the wild.
27	If required the Bidder should be able to assist for an incident response, from the initial detection to the final resolution of the incident.
28	The bidder must able to provide Signatures, YARA rules, detection rules, block rules for the solution deployed in Bank environment such AV, SIEM, EDR, IDS/IPS, NBAD, AD, etc. in order to detect the presence of IOC or revert the back the changes made by the attacker.
29	Bidder must be able to perform non- intrusive IR activities such as log collection, scanning activity, IOC scans using inbuilt tools in cases if agent installation or vendor proposed tool installation is not possible.

Broad Scope of work for Cyber / Digital Forensics:
The primary scope is to provide Digital / Cyber Forensic and Incident Investigation services to Indian bank. These services may encompass (but not limited to) Evidence collection, acquisition of data, imaging, examination, recovery and presentation of digital evidence for legal admissibility as determined by Indian bank on need basis.

C) Scope for Cyber / Digital Forensic Readiness Assessment:

As a part of the assessment of the Cyber/Digital Forensic Readiness of the Bank, the vendor after review of the existing Infrastructure of the Bank has to provide an assurance / confirmation to the bank that functioning of the Bank's IT system is in Compliance with –

- Bank's Cyber Crisis Management Plan
- RBI Information Security guidelines, Cert-In guidelines, any other legal requirements.

The vendor should benchmark the Bank's Cyber Crisis Management Plan and IT Data Backup Policy with industrial standard and Government regulations and report the identified gaps / non-compliance.

Initially on the first year of appointment, the Vendor shall conduct Digital/Cyber Forensic Readiness Assessment of Bank's IT Infrastructure in order to analyse, identify and mitigate the deficiencies, if any, in the Forensic Incident handling, Evidence collection and storage capabilities, with provision for yearly review of the findings for the next two years. Yearly review of the Bank's critical IT infrastructure, including revalidation of gaps identified to be done and in case of any changes in the Bank's Digital IT Infrastructure/Environment within the period of engagement (3 years) subsequent to the conduct of initial/previous year assessment after engagement, as intimated by the bank, the Vendor shall be required to reassess the Digital/Cyber Forensic readiness for those Business functions/Applications/Devices and submit report at no extra cost to the Bank. Gaps identified during the yearly assessment has to be closed after revalidations within 3 months of submission of final report of that year.

Deliverables shall include but not limited to provide detailed report at the time of assessment of forensic readiness covering the following aspects:

- Review of network architecture and extant critical business applications
- Review of sufficiency of existing log collection, log retention/Backup/archival processes, Policies /Procedures etc. for network & security devices such as Firewall, Routers, Switches, SIEM etc. and Bank's business applications.
- The vendor shall evaluate various areas of security in a multi layered approach (Web, App, DB layers, network security etc.) covering incidents related to CBS, RTGS, DLP, HR Connect, SWIFT, all alternate delivery channel products (Internet Banking, Payment Banking, Mobile Banking, ATM etc.) and any other product / applications being used by the Bank.
- Review the existing Cyber Incident Handling capabilities in terms of People, Process and Technology
- Identify available sources and sufficiency of different types of potential digital evidence for the identified devices and business applications.
- Identify the additional sources of logs that need to be captured to ensure completeness for conducting incident investigation and this includes the formats of logs and whether they contain meaningful information for investigative purposes and admissible in the court of law.
- Evaluate the procedures followed by IT teams to make the necessary evidence available for investigation.
- Evaluate whether the captured logs are in totality on a sample basis and also validate the basis for selection of samples.
- Identify and validate the procedures carried out by IT team to securely gather legally admissible evidence to meet the Legal, Regulatory requirements such as Cert-In, RBI, NCIIPC etc.
- Collate the information obtained through deep dive analysis and submit a gap analysis report.
- Remediation advisory guidance
- Provide onsite training /awareness to Bank's designated personnel (Minimum 10) in the area of Digital/Cyber Forensic Investigation & related topics in the first year.

The outcome of the overall assessment should enable the bank in:

- Ensuring the overall integrity and continued existence of an organization's computer system and network infrastructure.
- Helping the organization by preparing detailed forensic reports for internal use and legal proceedings. Provide expert testimony in court/regulatory hearings.
- Tracking complicated cases like cyber-attacks, such as Data Theft, Data Leakage, Insider Fraud, Malware attacks, APTs, Ransomware attacks etc.
- Investigate financial fraud and unauthorized transactions committed using digital resource.
- Assessing the effectiveness of its defences and incident response strategy whilst not limited to technical controls.

- Raising awareness of our security team's inherent strengths and weaknesses. This information will make informed decisions concerning Bank's security strategy.
- Helping the organization develop "battle-hardened" defences against Advanced Persistent Threats (APT), Ransomware etc.
- Testing the effectiveness of our Incident Response plans and challenge our team's breach detection capabilities.
- Assisting with identification of High Value Targets (HVTs) and weaknesses based on common methodologies. HVTs could be People, Systems, Processes or Technology.
- Provide assurance report to Bank that Bank is prepared/ready for Digital/Cyber Forensic Readiness covering all network and security devices, applications, concerned servers etc deployed in the Bank. This assurance has to be provided based on full assessment of Bank's network as per scope.
- Recommend improvements to security policies/cyber crisis plan based on forensic findings.

D) Scope for conduct of Cyber/Digital Forensic Incident Audit/ Investigation/ Analysis (but not limited to):

- Methodology for reporting findings of analysed data and making the information available for review through a secure online portal. The timeframe for storage of report findings to be mentioned.
- An end-to-end investigation tracks all elements of a suspected compromise, including how the compromise initiated, which devices/systems were compromised, and the associated recovery process.
- Should be able to provide cyber forensic services including (but not limited to) the examination of computers, mobile phones and other digital devices, digital evidence preservation, recovery, analysis, electronic mail extraction and database examination.
- Undertake Digital & Mobile Forensics including indexing of complete data, timeline analysis, meta data analysis, Decryption and password cracking, keyword searching, data retrieval etc.
- Perform Cyber forensic investigation of varied operating systems (but not limited to) Windows, Linux, UNIX, Mac OS, Enterprises OS etc.
- Perform Cyber forensics and Incident investigation of (but not limited to) web/client based applications, databases (Sybase, oracle, MS SQL, Postgress etc.)
- Perform cyber forensics and Incident investigation of (but not limited to) networking, email and security devices etc.
- To identify the malicious activities with respect to 5Ws + H (Why, When, Where, What, Who, How).
- Identify attack vectors by which a hacker (or cracker) could have gained access to a computer or network in order to deliver a payload or malicious outcome.
- Ensure that proper chain of custody (CoC) is maintained for integrity and all evidence recovery and collection methods are conducted, managed and achieved in a manner consistent to maintain preservation and protection of data and evidence in its original form such that it is admissible in the court of law.
- It is expected to retrieve information stored on the devices in a form useful to investigator during legal/cyber investigation and business exigency.

- Prepare and submit detailed forensic report on the technical and executive aspect of the investigation.
- Create and maintain an electronic audit trail or manual record of all processes, including work-papers, applied to gather and examine relevant evidences in such a way to ensure even third parties should be able to examine those processes and achieve the same result.
- Collection and Preservation of Electronic Evidence
- Data Recovery and Analysis
- Analysis of User/Malicious Activity
- Handling Password Protected Files
- Data Forensic Investigation
- Expert Testimony
- Secure Shipments, in case of need
- Chain of Custody Management
- Ability to meet the service levels.
- Ability and experience in providing IT Forensic and e-Discovery services to harvest data from IT security devices.
- Ability to provide services related to restoration of backup systems, including enterprise-wide backup systems.
- Ability to provide services related to restoration of corrupted, deleted, hidden, and encrypted or temporary data.
- Ability to provide services related to restoration of damaged media.
- Ability to provide services related to restoration of password protected files.
- Ability to have methodology for collecting data, including volatile data.
- Ability for preserving metadata during data capture with the goal of preserving the evidentiary value and the chain of custody.
- Conduct digital forensic analysis with various models, as and when incidents (which triggers forensic analysis as per the bank policy) happen.
- Methodology for analyzing preserved and collected data.
- Providing in detail the gaps in the existing security controls used to protect the data on banks premises and during transmission, transfer of Bank’s data etc.
- Provide a sample of the types of logs that are created in the device throughout the review process and describe the process by which they are created.
- Detail the existing controls for secure transmission, transport, and shipment of Bank’s data and your procedure used to protect the confidentiality and integrity of such data
- Information about the incident type and its modus operandi
- Description of how the incident was discovered.
- Information about the systems that were affected.
- Information about who was responsible for the system and its data.
- A description of what caused the incident.
- A description of the response to the incident and whether it was effective.
- Recommendations to prevent future incidents.
- A discussion on lessons learned to improve future responses.
- A timeline of events, from detection to incident closure

- Identify available sources of potential evidence in the environment, including: Email, Network traffic, logs, and archives, User documents, media, and voice mail, social media, Smart Mobile devices, Cloud Services, Smart devices, etc.

- Identify and validate the procedures carried out by IT team to securely gather legally admissible evidence to meet the Legal Regulatory requirements.
- A POC of replaying/reconstructing the same incident on test environment, proving the analysis is right.
- Reconstruct timelines and attack vectors, for demonstration to the Bank when necessary.
- Recover deleted, encrypted, or damaged data from Critical Systems including cloud (Private), when required by the Bank.
- Should support the Bank in identifying the attack simulations performed by the regulators and third-party vendors in the event of Cyber Drill Exercise.
- Must have the ability to perform malware analysis and reverse engineering of malware samples using both automated and manual techniques and provide host-based and network-based indicators that are used to find the malware variants.

The vendor should ensure that the following rules are upheld during an investigation:

- No possible evidence is damaged, destroyed, or compromised by the forensic procedures used to investigate the computer (preservation of evidence).
- No possible computer malware is introduced to the computer being investigated during the analysis process.
- Any extracted and possibly relevant evidence is properly handled and protected from later mechanical or electromagnetic damage (extraction and preservation of evidence).
- A continuing chain of custody is established and maintained (accountability of evidence).
- Normal operations are affected for a very limited period of time, if at all (limited interference of the crime scene on normal life).
- Details of the client-attorney relationship are not disclosed if obtained during a forensic process in order to maintain professional ethics and legality (ethics of investigation).

Vendor should guide electronic discovery and investigative processes, providing Bank's legal teams with sound advice and an expanded source of evidentiary techno legal information acceptable at judiciary platforms. Vendor should be able to carefully analyse the details of each case to conduct timely and thorough investigations to extract techno legal evidences acceptable at judiciary platforms.

The appointed vendor will conduct a desktop exercise upon appointment to guide bank stakeholders on the vital first steps to take during any incident.

The appointed Digital/Cyber Forensic vendor is expected to:

- Define the business scenarios that will require digital evidence collection.
- Reducing the impact of computer-related incidents.

- Guidance on ensuring compliance with regulatory or legal requirements.
- Determine evidence collection requirements and procedures.
- Establish evidence collection procedures that are legally admissible in court.
- Establish a policy for secure storage and handling of potential evidence.
- Facilitate training and understanding of security incidents and detection across the Bank network.
- Review and provide guidance within defined SLAs to reduce potential revenue losses and recovery of the same.
- Recommend changes to methodologies while minimizing negative customer impact.
- Represent the Bank in a court of law, as and when required, to substantiate their findings and provide supporting evidence and support Bank's legal council if necessary in this regards.

Broad Scope of work for RED TEAM EXERCISE:

III. <u>BROADER PROJECT SCOPE:</u>

- The Security Service Provider to conduct the Red Team Exercise to uncover the vulnerabilities in the bank's perimeter/ internal network (DC/ DR/NDR and on sample basis for branches/Offices and attempt to exploit the identified vulnerabilities to gain access to the bank's Critical Infrastructure like Servers, Databases, Network devices and Security Appliances.
- In order to enhance Information Security Posture of the Bank and to defend Bank against outside/internal threats Bank needs to carry out Red Team Exercise through the bidder to know various attack tactics and the methods to defend against such attacks.
- Red Teams will act proactively by simulating real attacks and attempt to penetrate security controls undetected. Their role is to highlight loopholes in Security Control and to improve detection, response, recovery and mitigation capabilities for Blue Team - SOC and IT operations.
- The impact on network performance should be minimal during Red Team Exercise and should not impact any normal user flows. Non-Destructive simulation Initiator would only be allowed to generate lightweight traffic. Tests in the production network should not be destructive - destructive behaviour tests are only done in the secure containers, a sandbox separated from the production network.
- The Red Team Exercise should provide information and guidance on remediation of identified results. The Red Team Exercise should provide ample information on the specifics of each attack in order to enable INDIAN BANK Security Operation Centre (SOC) Team and different other Teams (Network, Endpoint, Email, Data Centre, CBS etc.) to remediate any issues encountered.
- The Red Team Exercise should support testing email security controls against data exfiltration, malware, phishing etc.. It should enable the validation and tuning of INDIAN BANK's email security tools. It should leverage a dedicated internal and external email account destination to send threats like malware and spear-phishing links across the email server into INDIAN BANK, and to send sensitive information like PII and PCI data out of INDIAN BANK to validate that the email security and DLP controls in INDIAN BANK are in place are working as the Bank expects. This should support Office 365, Microsoft Exchange and other standard email Red Team Exercises.
- The Red Team Exercise should support executing external attacks from internet towards internal controls.
- The Red Team Exercise should support attack replay & attack import from PCA.
- Bidder is required to provide Red Team Exercise as a service only. However, required application, tools or any other appliance if required to conduct the Red Team Exercise

to be arranged by the bidder at their own cost and to be deployed and used within the Bank's premises in presence of Bank Officials.

IV. DETAILED SCOPE OF WORK

The Red team exercise should involve the full attack lifecycle, from initial reconnaissance to mission completion. The objective is to test and validate the ability to detect malicious activity and evaluate the response to the detected events. The Red team exercise should provide an accurate situational awareness of the security posture of a given system/network. The Red Teaming exercise must essentially include the undernoted phases:

Category	Activities
Reconnaissance	Passive scanning, OSINT gathering, domain enumeration, email harvesting
Initial Access	Phishing, watering hole attacks, exploiting public-facing apps, USB drops
Execution	PowerShell abuse, macro-enabled documents, scheduled tasks
Persistence	Registry run keys, startup folder implants, service creation
Privilege Escalation	Token manipulation, exploiting vulnerable drivers, bypassing UAC
Defence Evasion	DLL sideloading, obfuscation, disabling AV/EDR, clearing logs
Credential Access	LSASS dumping, keylogging, brute-force, credential spraying
Discovery	Network mapping, AD enumeration, identifying security controls
Lateral Movement	Pass-the-Hash, RDP hijacking, SMB exploitation, remote WMI
Collection	File scraping, clipboard monitoring, screen captures
Exfiltration	DNS tunnelling, HTTPS uploads, cloud sync abuse
Command & Control (C2)	Custom C2 frameworks, encrypted channels, domain fronting
Impact Simulation	Ransomware deployment (in isolated test), data corruption, service disruption

A. SCANNING PHASE :

i. Conduct ping sweep scans and identify the reachability of IP segments.
ii. Identify live IP addresses within the identified IP segments.
iii. Launch stealth/noisy scans on the bank's IP addresses and identify open & vulnerable ports.
iv. Intelligence gathering by Passive Reconnaissance to extract sub domains, hosts.
v. Identify IP ranges and vulnerabilities in publicly available server/network devices & internally.

B. FINGERPRINTING/ VULNERABILITY IDENTIFICATION PHASE.

i. Detecting TCP/UDP services and version details
ii. Detecting Operating systems and its version details using active and passive OS fingerprinting techniques without any impact on the production environment.
iii. Fingerprinting web servers and HTTP/ HTTPS services running on the bank's internal and external servers.
iv. Attempt to identify weakly configured web applications/ web servers/ Operating systems/ databases
v. Attempt to identify vulnerabilities in network services, operating systems, and Network devices using combination of advanced vulnerability scanners and

manual tests.

vi. Script scan to identify potential vulnerabilities.

vii. Identify vulnerabilities in external facing web applications with Black Box approach.

viii. Identify potential exploits available for identified vulnerabilities using well known exploitation framework modules.

C. EXPLOITATION AND POST EXPLOITATION PHASE

This phase will include exploitation of the identified vulnerabilities in operating systems, web applications and network services. Post exploitation phase may include attempts to execute following key attacks in a controlled environment as applicable:

i. Gain access to the underlying operating system

ii. Evaluate the potential for gaining further access to the bank's internal network

iii. Extract credentials and password hashes from operating systems memory

iv. Exploiting OS misconfigurations and local process vulnerabilities to gain privileged access on target server

v. Attempt to identify if a device, web application is vulnerable to a default credential attack. vi. Attempt to exploit vulnerabilities in network/web services using exploitation frameworks and publicly available exploit codes as applicable.

vi. Examining Bank for weaknesses as through the eyes of an industrial spy or a competitor or attacker using following techniques:

v) Password Cracking, and Bypassing Windows User Account Control (UAC)

w) PowerShell exploitation, Pass the hash

x) Lateral Movement

y) Network Domination & Persistence

z) Network Infrastructure including end points and servers exploitation for cases such as Firewall bypass, Router testing/ configuration, DNS foot printing, Proxy Servers, Vulnerability exploits, Misconfiguration exploits

aa) Evasion & Obfuscation Techniques

bb) Data exfiltration - Internal network, External network, Storage device

cc) Attacking Linux/Unix Environments

dd) Privilege Escalation to obtain root privileges

ee) Virtualization Attacks

ff) Web application compromise and exploitation – physical and Cloud

gg) Social Engineering Attacks (Spear phishing, Phishing,Vishing)

hh) Carry out DDos attack exercise

ii) Evade proxy rules

jj) Covert channel call-backs

kk) Local privilege escalation

ll) Lateral network scans within and across subnets

mm) Discover and access file shares

nn) Horizontal brute force attacks

oo) Brute force - Security appliances

pp) Attempt to access - Remote branches, DMZ, Internal servers, Core Servers

D. SOCIAL ENGINEERING

Human interactions typically gain unauthorized access to systems or information that may result in system or network intrusion or disruption. The vendor shall be responsible for

conducting social engineering attack (targeting employees through “Vishing” ,”Phishing” etc.) to assess the level of employee awareness in terms of cyber threats.

The common attack vectors include malicious emails, phone calls, removable media and physical penetration testing.

- ✓ External exposure of the Company
- ✓ Effectiveness of security awareness efforts
  - USB drop exercise
  - Through social media
  - Phishing
  - Vishing
  - SMShing etc.

E. TRAINING

Vendor is required to impart training to the identified bank personnel/ SOC team on the Red Team Exercise with use cases, analysis and resolution of the red team exercise carried out, functionality and services. In addition to that, mandatory training is to be provided to Bank staff yearly after completion of the activity for handling the guidance as Blue team against Red Team Exercise. Time to Detect & time to respond matrix should be prepared for the Bank to review the blue team performance.

F. RED TEAM ASSESSMENT

The Service Provider is required to deliver Red Team assessment with below specifications and actions:

a) Service Provider must use non-destructive methods necessary to accomplish a set of jointly agreed upon mission objectives while simulating attacker behaviour.

b) Scope of the assessment must cover the internal security team's ability to prevent, detect, and respond to incidents in a controlled and realistic environment against
   - Technology - Servers, Databases, Security & Networks, Applications, Routers, Switches, Appliances
   - People - Staff, Outsourced Vendor Personnel, Departments, business partners
   - Physical Facilities - Offices, Data Centre, Disaster Recovery Site

c) The Service Provider must closely mimic a real attacker's active and stealthy attack methods by using Technic, Tactics and Procedure (TTP) seen on real, recent incident response engagements in order to assess the security team's ability to detect and respond to an active attacker scenario. The service provider shall conduct red team exercise to focus on giving the bank’s security teams a practical experience combating real cyber-attacks to simulate the tools, tactics and procedures (TTPs) of real world attackers that target our environment, while avoiding business damaging tactics.

d) Vendor must adopt fact-based risk analysis and recommendations approach.

e) The engagement must follow the phase of attack life cycle which minimally should consist of Initial Compromise, Establish Foothold, Lateral Movement, and Complete Mission.

f) Bidder must leverage a combination of proprietary intelligence repositories as well as industry leading commercial threat intelligence tools and techniques throughout the engagement.

g) The scope of engagement will include testing of the bank’s detection and response capabilities.

h) From the samples provided, the bidder should be able to differentiate genuine and suspected fraudulent behaviour.

i) The red team exercise should cover a wide spectrum of applications, browsers, databases, web servers and other components.
j) Identify gaps in IT Perimeter security devices such as Firewall, WAF, NIPS, Proxy, EDR, HIPS and network segmentation.
k) ATM, Kiosk compromise simulation
l) Mobile App & Web portal attacks
m) Insider Threat Simulation
n) Swift Network Simulation
o) In case of each simulation, there should be feature for rollback wherever required.
p) Testing the incident response mechanism of the bank to identify the capability of the bank in breach readiness and thus Improve the organizational incident handling and recovery mechanism to 'restore the business in time' at the time of real cyber-attack.
q) Utilizing the existing security flaws to gather more information, owning the system, network, application etc.
r) Conducting controlled exercise to challenge the existing defending control system to get inside the organization by physically/logically/social means.
s) Should be able to demonstrate mitre attack framework to the Bank.

G. TOOLS

The service provider to ensure that the tools or any software used for conducting the assessment is fully licensed and property of the service provider. Any software or tool to be installed in any of the devices in Banks network or premises has to be done by the service provider by taking necessary permission and licenses, if any. The software or tools installed for the assessment have to be removed once the activity is over or the contract is terminated.

The necessary tool/software should be brought by the bidder installation in Bank's Premises only and should be customizable as per the scope of work.

Indicative list of custom attacks includes but not limited to:

- DNS requests
- Custom email (attachments, links in body, etc)
- Web requests
- Socket
- Host CLI for endpoint (python, bash, windows CMD, powershell)
- TCP Port Scan
- MITM attack (Man-in-the-middle)
- DNS redirection
- SQL Injection
- Web Defacement
- Password Brute Force
- Cross site scripting etc.

H. DELIVERABLES

The service provider should provide detailed test reports covering the following aspects at minimum:

- Executive summary

- Test methodology
- Observations
- Findings, Root causes
- Recommendations

After each Red Team Exercise, deliverables (supporting documents/ evidence) in relation to analysis should be reported/ submitted to the bank highlighting the findings and steps for mitigation of the same after completion of the exercise broadly covering the below aspects.

6. Detailing the Security Gaps:

Technical report of red team attack for each phase wise:

The deliverables need to include an electronic report that includes several key components, but not limited to:

- Control framework (i.e OWASP, PCI, PTES, OSSTMM).
- Summary of open-source intelligence (OSINT) gathered from internet and dark web
- Methodology and approach
- Target list created by OSINT
- Review of sensitive company data discovered on internet.
- Results of the assessment (description, business impact, recommendation, evidence, references, CVSS, risk rating, etc.)
- In addition to the electronic report, a raw file in comma-separated value (excel or CSV) format should also be provided in an effort to optimize the remediation and management of any identified findings.
- Detailing the System setup and tools used, and the tests conducted during the exercise.
- Analysis of the findings and document the security gaps such as vulnerability, configuration flaws, security flaws, gaps identified, threats etc. observed during the testing activity as per the scope of work.
- Document recommendations and Exercises for addressing the identified security gaps and categorize the identified security gaps based on their criticality.
- Chart a roadmap for the Bank to ensure compliance and address these security gaps.

7. Addressing the Security Gaps:

- Recommend actionable fixes for systems vulnerabilities in design or otherwise for application systems and network infrastructure. If recommendations for Risk Mitigation/ Removal could not be implemented as suggested after discussion with Bank, alternate compensatory controls to be provided.
- Suggest changes/modifications in the Security Policies implemented along with Security Architecture including Network and Applications of the Bank to address the same.

8. Summary of Final Report:

Summary of exercise findings including identification tests, tools used, and results of tests performed.

- Tools used and methodology employed.
- Positive security aspects identified.
- List of vulnerabilities identified with POC /supporting Evidences.

- Description of vulnerability
- Risk rating or severity
- Category of Risk: Critical / High / Medium / Low
- Methodology/Test cases used in exercises.
- Illustration of the test cases

9. Exit Meeting

Findings are to be communicated effectively in a stakeholder meeting and typically presented in person. During this time, red team security consultants should walk through the report, in detail to ensure all findings and their corresponding description, risk rating, impact, likelihood, evidence and remediation steps are thoroughly understood. While this typically involves a single meeting, there is no limitation to that number. The key aspect should be that all information is clearly understood and that a roadmap towards remediation/mitigation is clear.

After review, the service provider has to provide confirmation to the bank that functioning of network system is in compliance with

- Bank's Information Security Policy
- Bank's Cyber Crisis Management Plan
- RBI Information Security guidelines and Framework, CERT-In guidelines, any other legal requirements etc.

10. Remediation and re-testing

Remediation re-testing to be provided at no additional cost after compliance.

J. Systems presently prevailing in the Bank:

- Networks - Bank has a WAN setup connecting all the branches and offices PAN India using MPLS, VSAT, etc. The routers and switches used are of standard OEM models. The main core banking application is "Bancs". SWIFT application is also used in our setup. Delivery channels like ATMs (Onsite & Offsite), Internet & Mobile Banking, RTGS, NEFT, UPI and Financial Inclusion also form part of the network. Bank has major network and security solutions deployed in the network.

- People - Some of the IT operations are handled by Bank staff and some are outsourced to vendor personnel who are located in the premises within the Bank/Data Centre.

- Physical Facilities - Bank's Data Centre is located at third party Data Centre provider location. Our main IT department is located at Head Office in our own premises. Various other departments are also located in our own premises.

K. Other general requirements

The service provider should benchmark the policies, procedures/processes, standards against the standards recommended by RBI and identify gaps. The service provider should report on the areas where they have observed the bank to be non-compliant with the RBI guidelines.

The outcomes of the overall exercise should enable the bank to:

- Assess the effectiveness of its defenses and incident response strategy whilst not limited to technical controls.
- Provide a real-world cyber war/training opportunity and defend against a live attack.
- Raise awareness of our security team's inherent strengths and weaknesses. This information will make informed decisions concerning our security strategy.
- Help the organization develop defences against Advanced Persistent Threats (APT).
- Test the effectiveness of our incident response plans and challenge our team's breach detection capabilities.
- Assist with identification of High Value Targets (HVTs) and weaknesses based on common methodologies. HVTs could be People, Systems, Processes, Technology.

Broad scope of work for conducting Cyber Drill:

1. Purpose

The purpose of this engagement is to conduct a practical, hands-on cyber drill to test the bank's resilience to cyberattacks, identify gaps in its incident response capabilities, and enhance the technical skills of the security team. The ultimate goal is to validate and improve the bank's cyber security posture, ensuring full compliance with the regulatory Framework.

2. Phases of Engagement

Phase 1: Planning and Scenario Design

- Initial Consultation: The expert team will hold a kickoff meeting with key bank stakeholders to understand the current security landscape, existing controls, and specific concerns.
- Threat Scenario Development: The expert will design a realistic, multi-stage cyberattack scenario. This will not be a simple vulnerability scan but a narrative-driven attack, simulating initial compromise, lateral movement, and a final objective (e.g., data exfiltration or a financial system attack). The scenario will be tailored to the bank's environment and based on common threats in the financial sector.
- Rules of Engagement: A clear set of rules will be defined, outlining the scope, targets, and limitations of the drill to ensure no disruption to the bank's live production systems. The drill will be conducted in a controlled, isolated test environment.

Phase 2: Execution of the Drill

- Simulated Attack: The expert will execute the pre-designed scenario, acting as the "red team." This will involve using various techniques, including social engineering (e.g., simulated phishing), malware deployment in a test environment, and exploiting vulnerabilities to mimic a real attack.
- Active Defense: The bank's security team will act as the "blue team," using their existing tools and processes to detect, analyze, contain, and remediate the simulated threat. The drill will test their ability to identify IOCs (Indicators of Compromise), communicate effectively, and follow the pre-defined incident response plan.

- Observation and Data Collection: The expert will meticulously observe and document every step of the drill, logging the timeline of events, the actions of the blue team, and the effectiveness of security controls.

3. Deliverables

- Detailed Post-Drill Report: A comprehensive report will be provided, detailing the simulated attack timeline, a step-by-step breakdown of the blue team's response, and an analysis of their performance.
- Actionable Recommendations: The report will include a prioritized list of specific recommendations to improve the bank's cyber security. This will cover areas such as:
  - Process Improvements: Enhancements to the incident response plan, communication protocols, and a clear chain of command.
  - Technical Enhancements: Recommendations for new security tools, configuration changes, and patch management improvements.
  - Skill Gaps: Identification of training needs for the security team to better handle future incidents.
  - Executive Summary: A high-level, non-technical summary for senior management and the board, highlighting key findings, the bank's overall readiness score, and a high-level action plan.
  - Debriefing Workshop: A formal debriefing session will be held with all stakeholders to review the findings, discuss the recommendations, and plan the next steps.

Broad Scope of work for Tabletop Exercise (TTX):

Tabletop Exercise will be simulated, discussion-based incident response activity where key stakeholders in the Bank will walk through a hypothetical crisis scenario like any cyberattack, data breach, natural disaster etc to test their response plans, communication protocols, and decision-making without real-world disruption or technical execution.

Walk the participants through the scenario step by step:

h) Initial Trigger – What event or situation initiates the need for change? (e.g., sudden failure, new regulation, etc.)

i) Impact Assessment – What are the potential impacts of this change across systems, teams, and processes?

j) Risk Assessment – What risks are involved, and how can they be mitigated?

k) Stakeholder Analysis – Who are the impacted stakeholders, and how will they be communicated with?

l) Plan Development – Tell participants to draft elements of the CCMP (timelines, roles, resources, communication).

m) Execution and Monitoring – How will the change be implemented, and how will it be monitored?

n) Post-Implementation Review – What metrics will be used to assess the success of the change?

Tabletop assessment will be for following scenarios (but not limited to):

j) Ransomware

k) Compromise of Critical System

l) DOS & DDOS Attacks

m) Data Breach/ Leakage/ Exfiltration (external)

n) Malware attack at critical setup like DC/DRS

o) Defacement of websites

p) Third party service provider compromised

q) Crown Jewel IT Asset corrupted/ failed

r) Major failures of Network at DC/DRS

Primary Objectives of a Tabletop Exercise:

i) Validate Incident Response Plans

j) Clarify Roles and Responsibilities and Confirm that each participant (technical, legal, PR, HR, etc) understands their duties during an incident.

k) Test internal communication channels and escalation processes across teams and different departments.

l) Improve Decision-Making Under Pressure

m) Identify Gaps in People, Processes or Technology

n) Test Regulatory and Legal Readiness

o) Assess how the organization handles breach notification, compliance and interaction with regulators or law enforcement agency.

p) Increase Organizational Awareness and Resilience in operation and technology

2) Timeframe for completion of activities

Bidder shall be responsible for the complete delivery, installation, implementation and maintenance of the services as per the timelines mentioned in the table below. Any breach in the timelines shall lead to imposition of penalty.

S.No.	Milestone	Timeline
1.	Incident Response Readiness Assessment (IRRA)	Within 60 days from date of Purchase Order
2.	Cyber/Digital Forensic Readiness Assessment	Within 60 days from date of Purchase Order

3.	Review of Incident reporting mechanism of Bank	Within 60 days from the date of Purchase Order
4.	Red Team Exercise	Within 1 year from the date of Purchase Order
5.	Tabletop Exercise	Within 1 year from the date of Purchase Order
6.	Cyber Drill	Within 1 year from the date of Purchase Order
7.	NDA/SLA/Contract execution	Within 30 days from the date of Purchase Order

8.	**Incident Response services initiation timelines**:		
	S.No.	Initial response 24*7*365 days support facility for incident response	Upper time limit
	1.	Incident's initial response and containment once alerted from Bank through call/email/message/any other communication medium for any location.	4 hrs
	2.	Once the incident is confirmed, the IR analyst must start working on preliminary information submitted by the Bank IR support.	6 hrs
	3.	Onsite location support – Incident response analyst should be available in the location of incident whenever needed	
	3.1	Within Tier -1 cities, metro cities & state capitals of India	12 hrs
	3.2	Within India- Other than above mentioned cities in 3.1	24 hrs
9.	**Incident resolution and restoration timelines:** 6. Critical Incidents must be resolved within 02 days. 7. High Severity Incidents must be resolved within 04 days. 8. Medium Severity Incidents must be resolved within 07 days. 9. Low severity incidents must be resolved within 10 days. 10. For specific type of incidents such as ransomware attack, data breach and phishing attack shall be decided, defined & mutually agreed between Bank and Bidder in the SLA.		
10.	IR support vendor shall submit comprehensive incident report within 24 hours from incident resolution & restoration to Bank.		

*Immediate remedial action should be taken upon flagging of observations / vulnerabilities having critical and high rating without waiting for final report.

3) Liquidated Damages (LD)

If the Supplier fails to deliver any or all of the Goods/Services or to perform the Services within the period(s) specified in the order, for reasons solely attributable to the Supplier, or the goods fail to perform to desired efficiency/ standards/ functionalities, then Purchaser shall, deduct from the relevant order price, as liquidated damages, Rs.10,000/- for the

delayed Goods/ Services for each day or part thereof of delay until actual delivery/completion of services, up to a maximum deduction of 10% of the total cost outlay of respective services for a period of three years. Once the maximum is reached, the Purchaser may consider termination of this order.

4) Payment Terms

1.	**Payment schedule**	**On completion of Incident Response Readiness Assessment (IRRA) (i.e., Phase 1):** Payment would be made against raising of invoices, along with submission of all relevant documents or deliverables.
		On completing Incident Response Process: On actual deployment/usage of IR services, an invoice for actual Hours/Man-day utilized for incident response can be processed upon satisfactory completion of each incident response.
2.	**Payment schedule**	**On completion of Digital/Cyber Forensic Readiness Assessment:** Payment would be made against raising of invoices, along with submission of all relevant documents or deliverables.
		On completing Cyber/Digital Forensics Incident Audit / Investigation / Analysis: On actual deployment/usage of Forensic services, an invoice for actual Hours/Man-days utilized can be processed upon satisfactory completion of each case.
3.	**Payment schedule**	**On completion of Red Team Exercise, Tabletop Exercise and Cyber Drill**: Payment would be made against raising of invoices, along with submission of all relevant documents or deliverables.

***** Payment will be made yearly in arrears, after completion (on acceptance by Bank) of services.

Note:

I. TDS on payments will be deducted as applicable.
II. All the payments will be made to bidder electronically in Indian Rupees only. Payment will be made against delivery invoices and challans duly acknowledged by Bank officials.
III. Further, the above payments will be released only after submission of Accepted copy of Purchase Order, Performance Bank Guarantee, signing of SLA & NDA, Integrity pact by Successful Bidder.
IV. No advance payment will be made.
V. All the payments to the Bidder shall be subject to the report of satisfactory accomplishment of the concerned task / performance/ delivery of the Services to the satisfaction of Bank for this purpose.
VI. Penalties if any, on account of non-compliance of Service Requirements/ liquidated damages, if any, shall be deducted from the invoice value/ EMD amount.
VII. Under no circumstances Bank shall be liable to the Successful Bidder and/or

its employees/personnel/representatives/agent etc. for direct, indirect, incidental, consequential, special or exemplary damages arising from termination of the Contract.

VIII. Bank shall not have any liability whatsoever in case of any third-party claims, demands, suit, actions or other proceedings against the Successful Bidder or any other person engaged by the Successful Bidder in the course of performance of the Service.

IX. Bank reserves the rights to dispute/deduct payment/withhold payments/further payment due to the Successful Bidder under the Contract, if the Successful Bidder has not performed or rendered the Services in accordance with the provisions of the Contract which the Bank at its sole discretion adjudge.

X. Successful Bidder shall permit Bank to hold or deduct the amount from invoices, for non-performance or part performance or failure to discharge obligations under the Contract.

XI. It is clarified that any payments of the charges made to and received by Successful Bidder personnel shall be considered as a full discharge of Bank's obligations for payment under the Agreement.

XII. All out of pocket expenses, travelling, boarding and lodging expenses for the entire Term of this RFP and subsequent agreement is included in the amounts quoted in TCO and the Bidder shall not be entitled to charge any additional costs on account of any items or services or by way of any out-of-pocket expenses, including travel, boarding and lodging.

XIII. In case Bank extends Contract period, the tenure of the existing Performance Bank Guarantee shall have to be extended accordingly for the duration of contract extension and claim period of an additional 6 months. In case the same is not feasible due to any reason, Bidder shall have to submit a Performance Bank Guarantee of the same amount (10% of the Total Cost of Ownership) as submitted previously for the duration of contract extension and claim period of an additional 6 months.

5) Service Level

The Bidder shall have to enter into an agreement with Bank as per the terms and conditions of this RFP and it's subsequent Corrigendum/ Corrigenda.

The non-delivery of services or non-response or any breach of information will lead to penalty. The penalty is applicable in respect of non-delivery of services/ support as per the requirement of this RFP.

S.No.	Milestone	Frequency	Timeline	Penalty
1.	Incident Response Readiness Assessment (IRRA)	Annual	Completion of milestone within 90 days from the date of instruction from the Bank.	Penalty of Rs.5000 Per Day will be applicable, in case of delay.

2.	Cyber/Digital Forensic Readiness Assessment	Annual	Completion of milestone within 90 days from the date of instruction from the Bank.	Penalty of Rs.5000 Per Day will be applicable, in case of delay.
3.	Incident Response Support and Reporting	On Demand	RCA, Cyber Forensic report etc. to be submitted within 15 days, post reporting of incidence	Penalty of Rs.25000 Per Day will be applicable, in case of delay.
4	Cyber / Digital Forensics incident Audit / Investigation / Analysis and Reporting	On Demand	RCA, Cyber Forensic report etc. to be submitted within 15 days, post reporting of incidence	Penalty of Rs.25000 Per Day will be applicable, in case of delay.
4.	Red Team Exercise	Annual	Completion of milestone within 90 days from the date of instruction from the Bank.	Penalty of Rs.5000 Per Day will be applicable, in case of delay.
5.	Tabletop Exercise	Annual	Completion of milestone within 60 days from the date of instruction from the Bank.	Penalty of Rs.5000 Per Day will be applicable, in case of delay.
6.	Cyber Drill	Annual	Completion of milestone within 60 days from the date of instruction from the Bank.	Penalty of Rs.5000 Per Day will be applicable, in case of delay.

	Incident Response services initiation timelines:			**Penalty**
7	S.No.	Initial response 24*7*365 days support facility for incident response	Upper time limit	Penalty of Rs.10,000/- Per hour will be applicable, in case of delay.
	1.	Incident's initial response and containment once alerted from Bank through call/email/message/any other communication medium for any location and confirmation of incident.	4 Hrs.	

	2.	Once the incident is confirmed, the IR analyst must start live response analysis working on preliminary information submitted by the Bank IR support.	6 Hrs.	
	3.	Onsite location support – Incident response analyst should be available in the location of incident wherever needed		
	3.1	Within Tier -1 cities, metro cities & state capitals of India	12 Hrs. (Excluding travel time)	
	3.2	Within India- Other than above mentioned cities in 3.1	24 Hrs. (Excluding travel time)	
9.	**Incident resolution and restoration timelines:** 6. Critical Incidents must be resolved within 02 days, 7. High Severity Incidents must be resolved within 04 days. 8. Medium Severity Incidents must be resolved within 07 days. 9. Low severity incidents must be resolved within 10 days. 10. For specific type of incidents such as ransomware attack, data breach and phishing attack shall be decided, defined & mutually agreed between Bank and Bidder in the SLA. Criticality of incident will be decided mutually between Bank and Successful Bidder.			Penalty of Rs. 5,000/- Per Day will be applicable, in case of delay.
10.	IR support vendor shall submit comprehensive incident report within 24 hours from incident resolution & restoration to Bank.			Penalty of Rs. 5,000/- Per Day will be applicable, in case of delay.

WITNESS:

In witness whereof, the Parties have caused this agreement to be signed by their duly authorised representatives as of the date first written above.

For INDIAN BANK For M/s

Name: _____ Name:

GeM Bid Ref: GEM/2025/B/6707442 **Date:** ***20.09.2025***

Designation: _____ Designation:

Witness: Witness: