GeM Bid Ref: GEM/2025/B/6707442 **Date: *15.10.2025***

Bank has floated open tender by publishing the RFP in Bank's website and GeM portal for Selection and Appointment of service provider for Incident Response (IR), Cyber/Digital forensic services, Red Team, Tabletop & Cyber Drill Exercise (Ref: GEM/2025/B/6707442 dated 20/09/2025). In response to the pre-bid meeting held on 26/09/2025 and queries raised by the bidders related to RFP terms, please find the below clarification and amendments to RFP.

Response to the Pre-Bid Queries received for the RFP for Selection and Appointment of service provider for Incident Response (IR), Cyber/Digital forensic services, Red Team, Tabletop & Cyber Drill Exercise (Ref: GEM/2025/B/6707442 dated 20/09/2025).

New Clause (Table-1):

Sl No.	GeM Bid New Clause	Supporting Documents to be Submitted
1	**SECTION-II# 8.1** - Eligibility Criteria (RFP page No. 28) Below mentioned criteria added in the Eligibility criteria table: **S. No. 11 (added)** The Bidder or its subsidiaries should not be providing / have provided services to Indian Bank in the last TWO years in the following fields: a. Incident Response Services b. Forensic Services c. Security Solutions Implementation.	Undertaking on Bidders letterhead as per Annexure – XXI (attached)

Pre-Bid Queries & Response:

Sl No	Page No	Para No	GeM Bid Clause	Query/Queries Raised	Bank's Responses
1	Generic		Red Teaming Scope	Number of domains in scope.	The Red Team Exercise scope covers bank's Data Centre (DC), Disaster Recovery (DR), Network Disaster Recovery (NDR) locations, and sample basis for branches/offices as per RFP Section 4.2.1. The exact number of domains/subdomains will be determined during Rules of Engagement phase and kick-off meeting,

					however, the same keep on varying with addition of new applications.
2	Generic		Red Teaming Scope	Approx no of critical infra to be included in scope	Some of the Critical infrastructure includes Core Banking System, SWIFT network, ATMs (Onsite/Offsite), Internet Banking, Mobile Banking, RTGS, NEFT, UPI systems, servers, databases, network devices (routers, switches), security solutions & appliances (Firewall, WAF, NIPS, Proxy, EDR, HIPS etc) etc as outlined in RFP scope.
3	47	1	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	Approx no of critical infra to be included in scope	Some of the Critical infrastructure includes Core Banking System, SWIFT network, ATMs (Onsite/Offsite), Internet Banking, Mobile Banking, RTGS, NEFT, UPI systems, servers, databases, network devices (routers, switches), security solutions & appliances (Firewall, WAF, NIPS, Proxy, EDR, HIPS etc) etc as outlined in RFP scope.
4	49	Point No - Vi subpoint (m)	Carry out DDoS attack exercise	You want DDoS attacks to be carried out? Mention specific External Infra. At least count for now.	DDoS attack exercises are included in scope as per RFP Page 49, Point (m) and testing to be conducted in controlled manner to avoid business disruption on internet-facing infrastructures like Internet Banking, Mobile Banking, UPI, network and security devices etc.

GeM Bid Ref: GEM/2025/B/6707442 **Date:** ***15.10.2025***

5	49	Para No - D	USB drop exercise	You need Physical Assessment also? How many USB Drop you want to carried out?	Physical security assessment including USB drop exercises are part of Social Engineering scope as mentioned in RFP Pages 49-50. The USB drops have to be tested on sample systems/devices in at different locations across HO, CO, DC, DR and select branches/offices.
6		Para No - D	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.	No of employees to be included in training ? Is it physical or Virtual Training?	Training is mandatory yearly for identified Bank personnel/SOC team. The number of participants would be approx 15 officers and the mode of training (physical/virtual) will be decided by the Bank and communicated to the successful bidder.
7	Generic		Red Teaming Scope	Bank HO to Data Centre connectivity details. Need clarification. Is it IPSec Tunnel?	There is secure connectivity between Bank HO to Data Centre. Bidders must base their proposal on the general scope as further details on network architecture cannot be disclosed at this stage. Necessary details will be provided to the successful bidder upon NDA signing.

GeM Bid Ref: GEM/2025/B/6707442 **Date:** ***15.10.2025***

8	37	Point No - 6	2. 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.	Infrastructure should be in Banks premises or vendors premises? Also, retention period is of infrastructures or log/evidence's?	Infrastructure should preferably be in Banks premises or will be mutually decided with successful vendor. The retention period is of log/evidences.
9	37	Point No - 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:	Need more clarity what is the expectation ?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
10	39	Phase 4: Point No-1	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.	Logs for conducting DFIR which we collect are from proprietary tool hence logs are in proprietary format. relaxation on this point. We will provide help whenever needed	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
11	45	from top - point no 6,7,8	1. Ability to provide services related to restoration of corrupted, deleted, hidden, and encrypted or temporary data.	elaborate the expectation more.	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses

			2. Ability to provide services related to restoration of damaged media. 3. Ability to provide services related to restoration of password protected files.		mentioned in the RFP for detailed clarification.
12	46	Last point on the	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.	expectation is the vendor deputed lawyer will go to the court or vendor need to support the bank lawer ?	The findings and supporting evidences during digital cyber forensic analysis have to be represented by the bidder in a court of law, as and when required. This requirement is as per the relevant RFP sections and industry best practices.
13	28		Company incorporation (5 years)	Can bidders under Startup/MSME relaxation?	MSE/NSIC registered bidders are eligible for EMD exemption as per RFP Page 27. Documentary proof of valid MSE registration and declaration as per Annexure-VII must be submitted for claiming exemption.
14	28		Turnover requirement (₹15 Cr, ₹10 Cr for MSE/Startups)	Please confirm if turnover can be considered on consolidated basis for group companies or India entity only.	Minimum average annual turnover of Rs. 15 Crores (Rs. 10 Crores for MSE/Startups) from Indian operations of the bidding entity in three out of last four financial years (2021-22, 2022-23, 2023-24, 2024-25) as per RFP Page 29, Point 2.
15	28-29		Audited financial statements requirement	Will provisional balance sheet certified by CA be accepted for FY 2024-25 if audited financials are not ready?	In case, audited balance sheet is not available for 2024-25, the company may provide provisional balance sheet duly signed by Charted Accountant.
16	29		Experience requirement – IR/Retainer in PSU/BFSI	Please clarify if global BFSI references will be accepted in addition to Indian references.	Global BFSI references will not be acceptable as per RFP.

17	29-30		Certifications (SOC, ISO, GDPR, NIST etc.)	Please confirm if equivalent national certifications such as STQC, NIC, CERT-In empanelment will be accepted.	CERT-In empanelment is mandatory eligibility requirement as per RFP Page 30, Point 4. The bidder must have at least any one mentioned certification as per clause.
18	30-31		Minimum 10 resources with GIAC/EC-Council/OSCP etc.	Can bidders submit a mix of permanent and empanelled resources? At what stage (bid vs contract signing) should proof be submitted?	The bidder must have 10 resources with adequate skillsets mentioned in the RFP. The detailed proof have to be submitted during bid submission.
19	31		Litigation clause	Does the 'litigation threatening solvency' include civil disputes, tax disputes, or only bankruptcy/insolvency cases?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
20	31		Blacklist clause	If bidder was blacklisted more than 3 years ago but reinstated, will that be acceptable?	Bidder should not have been blacklisted/debarred/banned by Government/Government agencies/Banks/Financial Institutions/PSUs in India during last 3 years as per RFP Page 31, Point 7. Certificate as per Annexure-II required.
21	36		Incident Response Readiness	What is the expected volume of IR engagements annually? Is onsite presence mandatory for all incidents?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
22	36		Cyber/Digital Forensics	What type of cases are expected (endpoint, server, cloud, insider fraud,	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses

				mobile)? Please share indicative annual volume.	mentioned in the RFP for detailed clarification.
23	37		Red Team Exercise	Should the engagement be black-box, grey-box or white-box? Are phishing/social engineering/physical security in scope?	Bank aim is to get Red Team Exercise through the bidder to know various attack tactics and the methods to defend attacks by simulating real attacks and attempt to penetrate security controls undetected by the bidder. 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 bidder will be free to use all sort of attacks in cluding phishing/social engineering/physical security etc already provided in details in the RFP
24	37		Cyber Drills	Please clarify expected scale of cyber drill (branch level, pan-bank, or department wise). Is simulation platform required?	Cyber drills are scenario-based technical drills to test incident response mechanisms as per RFP Page 54. It will be as per Bank's discretion. Multi-stage attack simulations in controlled environment.
25	37		Tabletop Exercises	How many senior management stakeholders are expected to participate? Should vendor provide scenarios and facilitators?	Please refer to the clauses mentioned in the RFP for detailed clarification.

26	38		Deliverables	Please confirm if reports should follow RBI/CERT-In/IBA standard templates. Will the Bank provide its own template?	Regulatory framework references include RBI guidelines, CERT-In guidelines, and other applicable Indian regulations. Compliance reporting, if applicable/available, will be as per these frameworks. In other cases, Bank will discuss with bidder to finalize the reporting template.
27	125		Response Time SLA	Please confirm SLA clock start – from incident detection or from notification by Bank?	It will be reporting of alert from the Bank.
28	125		Forensic Report within 24 hrs	For complex incidents, can draft report be submitted in 24 hrs and final report within 5 working days?	Please refer to the clauses mentioned in the RFP for detailed clarification.
29	126		Penalty clauses	Are penalties applied per incident or cumulative for the quarter? Can bidder request a cap of 5% of annual contract value?	Please refer to the clauses mentioned in the RFP for detailed clarification.
30	32		Man-days assumption (15 IR, 15 Forensics)	Is this ceiling per year or indicative? Will additional man-days be separately payable?	Please refer to the clauses mentioned in the RFP for detailed clarification. On demand service, in case used, will be payable separately.
31	32		Reverse Auction	Please clarify whether L1 determination is based on RA final price or TCO including assumptions.	Please refer to the clauses mentioned in the RFP for detailed clarification.
32	33		Commercial Bid Format	Will Bank allow breakup between fixed annual charges and on-demand charges?	Please refer to the clauses mentioned in the RFP for detailed clarification.

33	58		Annual arrears	Request Bank to consider quarterly or milestone-based payments instead of annual arrears to support bidder cash flow.	Adhere to terms and conditions of the RFP
34	58		Ad-hoc incident response billing	Please confirm whether Bank will allow separate billing for incidents beyond bundled man-days.	Yes. For detail, please refer to the clauses mentioned in the RFP.
35	62		3-year contract	Please confirm if contract can be extended by mutual consent after 3 years without re-tendering.	Please refer to the clauses mentioned in the RFP for detailed clarification.
36	62		10% of contract value	Request Bank to consider 3% PBG as per latest GOI procurement guidelines.	Performance Bank Guarantee (PBG) of 10% of contract value is mandatory as per RFP terms. This is non-negotiable and required for contract execution throughout the 3-year contract period.
37	62		10% of contract value cap	Request Bank to cap LD to 5% of annualized contract value instead of total 3-year cost.	Adhere to terms and conditions of the RFP
38	Generic		Handover obligations	Please clarify if ongoing forensic investigations will be handed over to new vendor in case of termination mid-year.	Please refer to the clauses mentioned in the RFP for detailed clarification.
39	Generic		Prohibition of subcontracting	Please clarify if support from OEM/tool providers will be treated as sub-contracting.	The required services are expected from the bidder. The OEM/tool provider support shouild be taken of-line and they should not be supporting in Bank's sites. Please refer to the clauses mentioned in the RFP

					for detailed clarification.
40	Generic		Sharing reports	Can vendor share forensic/IR reports directly with regulators (RBI, CERT-In) when mandated by law?	Please refer to the clauses mentioned in the RFP for detailed clarification. In case needed, vendor may share forensic/IR reports directly with regulators (RBI, CERT-In) when mandated by la after taking permission from the Bank.
41	28		Bidder must be operating since last 5 years under Companies Act/LLP Act	Can bidders with proven BFSI cybersecurity track record but incorporated less than 5 years ago participate?	Please refer to the clauses mentioned in the RFP for detailed clarification.
42	28		Requirement for audited financial statements for 3 years	Will provisional balance sheet certified by CA for FY 2024-25 be accepted if audited statements are not available?	Yes. Please refer to the clauses mentioned in the RFP for detailed clarification.
43	36-37		Incident Response, Cyber/Digital Forensics, Red Team, Cyber Drill, Tabletop Exercises	Please confirm whether Bank expects onsite presence during IR/Forensic engagements or remote support is acceptable?	The support has to be onsite as per RFP terms and conditions.
44	36-37		Red Team Exercise – Simulated adversarial attacks	Should the Red Team engagements be black-box, grey-box, or white-box in nature? Please specify expectation.	Bank aim is to get Red Team Exercise through the bidder to know various attack tactics and the methods to defend attacks by simulating real attacks and attempt to penetrate security controls undetected by the bidder. 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 bidder will be free to use all sort of attacks as per detailed scope in the RFP
45	37		Cyber Drills (Annual/Biannual)	Please clarify expected number of participants and scope (technical drill vs. hybrid business-technical).	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
46	82-84		Requirement of being listed in Gartner/Forrester reports	Can equivalent recognitions, national awards, or BFSI references be considered instead of Gartner/Forrester listings?	Adhere to terms and conditions of the RFP
47	83		Requirement of more than 100 cyber incidents in 5 years with 10% BFSI	Can consortium approach or OEM-backed experience be counted to meet this requirement?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
48	125-126		Incident report submission within 24 hours post-resolution	For complex incidents requiring deeper forensics, can Bank allow draft report in 24 hours and final report within 5 working days?	Please refer to the clauses mentioned in the RFP for detailed clarification.
49	62		Contract term of 3 years	Please confirm if contract can be renewed/extended after 3 years without fresh tendering.	Please refer to the clauses mentioned in the RFP for detailed clarification.

50	62		Rs. 10,000 per day up to 10% of contract value	Request Bank to consider capping LD to 5% of annual contract value instead of entire 3-year cost.	Adhere to terms and conditions of the RFP
51	58		Yearly in arrears	Request Bank to consider milestone-based or quarterly payments instead of annual arrears to support cash flow.	Adhere to terms and conditions of the RFP
52	58		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.	The Bidder proposes to include notwithstanding any other provision in this RFP, the Bidder shall not be held liable for any third-party claims, demands, suits, actions, or other proceedings arising solely from the acts or omissions of the Bank, its affiliates, or its end users.	Adhere to terms and conditions of the RFP
53	58		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.	The Bidder proposes to include in the clause that any dispute, deduction, or withholding of payment by the Bank shall be based on objective and documented evidence of non-performance or material breach of contract terms by the Successful Bidder. The Successful Bidder shall be given a prompt written	Adhere to terms and conditions of the RFP

				notice detailing the specific deficiencies or non-conformities, and shall be given a reasonable opportunity to rectify such deficiencies within thirty (30) business days (Cure Period) before any payment is withheld or deducted.	
54	59		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	The Bidder proposes to incorporate that the Bank shall take prior permission from the Bidder before giving payment of charges to the Successful Bidder personnel.	The payment by the Bank for any services from the bidder will be done to their company name.
55	59		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.	The Bidder proposes to include that the Bidder or its employees shall have no liability if breach in service levels specified in the Agreement, meeting the specified timelines for provision of Services or failure or delay or non-delivery of Services or non – response is caused by the Bank or its employees in providing the necessary assistance required by the Bidder or its employees to	Please refer to the clauses mentioned in the RFP for detailed clarification.

				carry out the services, amendments, modifications, customizations, or alterations, the Bidder or its employees shall not be held liable and shall not be obligated to comply with the Implementation Plan and no penalty shall be imposed on the Bidder or its employees because of non-performance.	
56	62		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.	The Bidder proposes to include that the Bidder or its employees shall have no liability if breach in service levels specified in the Agreement, meeting the specified timelines for provision of Services or failure or delay or non-delivery of Services, Goods or non – response or the goods fail to perform to desired efficiency/ standards/ functionalities, is caused because of the Bank or its employees in providing the necessary assistance required by the Bidder or its	Please refer to the clauses mentioned in the RFP for detailed clarification.

				employees to carry out the services, amendments, modifications, customizations, or alterations, the Bidder or its employees shall not be held liable and shall not be obligated to comply with the Implementation Plan and no penalty or liquidated damages shall be imposed on the Bidder or its employees because of non-performance.	
57	63		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.	The Bidder proposes to include that 1.To the fullest extent permitted by the applicable law, in no circumstances shall Bidder be liable to the Bank, whether in contract, tort (including negligence and breach of statutory duty howsoever arising), misrepresentation (whether innocent or negligent), restitution or otherwise, for any incidental,	Adhere to terms and conditions of the RFP

				indirect, consequential, special or exemplary damages, punitive damages, loss (whether direct or indirect) of profits, business, business opportunities, revenue, turnover, reputation or goodwill (even if possibility of such damages were advised to that Party) in connection with its obligations under this RFP.	
				2. The Bidder shall have no liability for any damage caused by errors or omissions in any information or instructions, opinions, recommendations, forecasts or other conclusions provided to the Bidder or its employees by the Bank or its employees in connection with the Services or goods that are rendered under this Agreement.	

				3. The Bidder shall have no liability if breach in service levels specified in the Agreement, meeting the specified timelines for provision of Services or failure or delay is caused by the Bank in providing the necessary assistance required by the Bidder to carry out the services, amendments, modifications, customizations, or alterations, the Bidder shall not be held liable and shall not be obligated to comply with the Implementation Plan.	
58	63		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	The Bidder proposes to include 1. notwithstanding any other provision in this RFP, the Bidder shall not be held liable for any third-party claims, demands, suits, actions, or other proceedings arising solely from the acts or omissions of the Bank, its affiliates, or its end users.	Adhere to terms and conditions of the RFP

				2. The Bidder shall have no obligation under this clause or otherwise with respect to any infringement claim (a) based upon any use of the Deliverables not in accordance with this Agreement or for unintended purposes, or in violation of law; (b) based upon any use of the Deliverables in combination with other product, equipment, software, or data not intended by the Bidder to be used with such Deliverables; (c) that arises from any modification of the Deliverable by any person other than the Bidder (d) that arises out of or in relation to the negligence of the Bank and/or third parties other than Bidder or its employees.	

59	63		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.	The Bidder propose to delete this clause as it imposes absolute liability on the bidder in those circumstances also where the Bank or its employees are at fault.	Adhere to terms and conditions of the RFP
60	64		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.	The Bidder proposes to include 1. notwithstanding any other provision in this RFP, the Bidder shall not be held liable for any third-party claims, demands, suits, actions, or other proceedings arising solely from the acts or omissions of the Bank, its affiliates, or its end users.	Adhere to terms and conditions of the RFP

				2. The Bidder shall have no obligation under this clause or otherwise with respect to any infringement claim (a) based upon any use of the Deliverables not in accordance with this Agreement or for unintended purposes, or in violation of law; (b) based upon any use of the Deliverables in not intended by the Bidder to be used with such Deliverables; (c) that arises from any modification of the Deliverable by any person other than the Bidder (d) that arises out of or in relation to the negligence of the Bank and/or third parties other than Bidder or its employees. combination with other product, equipment, software, or data	
61	68		The Bank, without prejudice to any other remedy for breach of contract, by 90 days' written notice of default sent to the Supplier	The Bidder proposes to include that the Bank shall give ninety (90) business days to the Supplier to rectify the default before proceeding with Termination.	Adhere to terms and conditions of the RFP

62	78		The selected Bidder, during the term of the contract shall not without the express written consent of the Bank, directly or indirectly.	The Bidder propose to make this clause mutual.	Adhere to terms and conditions of the RFP. Bidder is not expected to express any information outside written consent of the Bank, directly or indirectly.
63	147		Notes	Bank the bidder request to include the process of raising the Invoice and the Bank shall pay the Bidder withing forty five (45) days of receiving the invoice from the Bidder.	Please refer to the clauses mentioned in the RFP for detailed clarification.
64	18 & 19		'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.	Pls brief - This is refered to own tools or propertiory Managed services platform owned by bidder	All tools and software must be commercially licensed and owned by service provider as per RFP Page 140. Any software/tools installed in bank's network require necessary permissions. Tools must be removed after assessment completion or contract termination.
65	29	8.1 (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. Privacy Shield	Our organization is CERT-In empanelled and currently holds an active ISO 27001:2013 certification. We are also in the process of transitioning to	CERT-In empanelment is mandatory eligibility requirement as per RFP Page 30, Point 4. The bidder must have at least any one mentioned certification as per clause.

			Frameworks or Indian equivalent certifications acceptable as per Bank's discretion. The bidder must be Cert-in empanelled.	ISO 27001:2022, with certification expected by January 2026. Kindly confirm whether our existing ISO 27001:2013 certification, along with CERT-In empanelment, will be acceptable under the Bank's discretion for the purpose of eligibility in this RFP.	
66	38	Phase 2	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.	As per the RFP, at least 2 IR analysts should be onsite within 24 hours (excluding travel time), if required. Kindly clarify whether this requirement is for permanent deployment of IR resources at Bank premises for the contract period (3 years) or only for deployment on demand during an incident, within SLA timelines.	24x7x365 availability required as per RFP Page 38. At least 2 IR analysts should be at onsite location (DC, DR, NDR, NDC, HO or CO) within 24 hours excluding travel time. Service provider must have minimum 10 relevant skilled resources with specified certifications.
67	132	Point 1	Deliverables shall include but not limited to provide detailed report at the time of assessment of forensic readiness covering the following aspects	Count of applications and infrastructure in-scope of the assessment.	Critical infrastructure includes Core Banking System (Bancs), SWIFT network, ATMs (Onsite/Offsite), Internet Banking, Mobile Banking, RTGS, NEFT, UPI systems, servers, databases, network devices (routers, switches), security appliances (Firewall, WAF, NIPS, Proxy,

					EDR, HIPS) as outlined in RFP pages 47-48. Along with this Bank has various other applications for different Banking operations.
68	30	8.1 (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 Certification (GREM) or • Computer Hacking Forensic Investigator (CHFI) or · Offensive Security Certified Professional (OSCP) • Certified Ethical Hacker (CEH)	Change the clause The bidder must have at least 10 relevant skillset resources on its payroll possessing at least any one of the following professional certifications	Adhere to terms and conditions of the RFP
69	27	7	Bid Security (Earnest Money Deposit)	We are a registered MSME organization and would like to request an exemption from the payment of the Bid Security (EMD) amount - 15,00,000/-, in accordance with applicable government provisions	MSE/NSIC registered bidders are eligible for EMD exemption as per RFP Page 27. Documentary proof of valid registration and declaration as per Annexure-VII must be submitted for claiming exemption.

70	38	Phase2- iii	Scope for Cyber / Digital Forensic Readiness Assessment	Kindly clarify whether the scope of on-premises services is limited to the Chennai location, or if additional locations are also included?	Services cover Chennai Head Office, Corporate Office, Data Centre, NDC, DRS (Mumbai), NDR (Mumbai) and sample branches as per RFP scope. Multi-location testing will be conducted based on bank's infrastructure spread across PAN India network.
71	42	7 A)	Scope for Cyber / Digital Forensic Readiness Assessment	Kindly clarify the exact number of applications, along with their critical components and critical infrastructure, that are expected to be covered under the specified services. Additionally, please confirm whether vendor-side applications are also included within the scope of assessment. This information is essential for accurately structuring our commercials.	Critical infrastructure includes Core Banking System (Bancs), SWIFT network, ATMs (Onsite/Offsite), Internet Banking, Mobile Banking, RTGS, NEFT, UPI systems, servers, databases, network devices (routers, switches), security appliances (Firewall, WAF, NIPS, Proxy, EDR, HIPS) as outlined in RFP pages 47-48. Along with this, Bank has various other applications for different Banking operations.
72	44	B- 10	Scope of Work - Cyber/Digital Forensics	Could you please clarify whether the chain of custody and evidence after collection will be maintained by the Bank or is expected to be maintained by us? Additionally, after data collection, should the analysis be performed at the Bank's premises, or can it be	Chain of custody must be maintained as per forensic standards mentioned in RFP Pages 44-46. Evidence analysis location should be within India to comply with data sovereignty requirements. All evidence must be legally admissible in Indian courts. Bank would prefer to have analysis at the Bank's premises.

				conducted at Deloitte's lab?	
73	57	5 -i - Payment Schedule	Payment Terms	Kindly clarify whether the HDDs required during the investigation will be provided by the Bank, or if we are expected to arrange for their procurement from our end.	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification. HDDs should be brought by the Bidder and if needed, Bank will have one copy of the same in its storages.
74	57	5 - Payment Schedule	Payment Terms	Should we raise the invoice for on-demand services upon completion, or would the Bank prefer a consolidated invoice at the end of the year?	Please refer to the clauses mentioned in the RFP for detailed clarification.
75	36	Section III- 1	Query regarding regulatory frameworks and reporting requirements	Please confirm the regulatory frameworks you want explicitly referenced in all deliverables and incident workflows: RBI Cyber Security Framework in Banks (2016), RBI Master Direction on IT Governance, Risk, Controls & Assurance (2023), CERT-In 6-hour incident reporting directions, SEBI Cybersecurity & Cyber Resilience	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.

				Framework, IT Act 2000 (Sections 43, 66, 72A), Indian Evidence Act Section 65B, and Digital Personal Data Protection Act 2023; also confirm preferred reporting paths, formats and approval flow for regulator notifications.	
76	4	3	At least 2 IR analyst should be at onsite location (DC, DR, NDR, NDC, HO or CO) of breach	Is there a minimum number of hours required per year	Please refer to the clauses mentioned in the RFP for detailed clarification. As per RFP clause, there are mandatory service and on demand service.
77	5	4,1	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	How long should the incident-related data be retained? Should the data be stored on the Bidder's premises or the Bank's premises	The duration of data retention and the secure storage location (Bank's premise or Bidder's secured premise) will be mutually decided with the successful bidder in accordance with RBI/Regulatory guidelines. Logs must be available for export in non-proprietary formats (Clause 5 Point 4.1).
78	8	3	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	Does DFRA include application readiness as well, i.e., checking if applications are capturing the required fields to answer the 5W's + H? If yes, please provide	Yes DFRA includes application readiness/analysis in a multi-layered approach. Critical infrastructure includes Core Banking System (Bancs), SWIFT network, ATMs (Onsite/Offsite), Internet Banking,

			(Internet Banking, Payment Banking, Mobile Banking, ATM etc.) and any other product / applications being used by the Bank	the list of applications for which DFRA is to be performed	Mobile Banking, RTGS, NEFT, UPI systems, servers, databases, network devices (routers, switches), security appliances (Firewall, WAF, NIPS, Proxy, EDR, HIPS) as outlined in RFP pages 47-48. Along with this, Bank has various other applications for different Banking operations.
79	12	I	The Security Service Provider to conduct the Red Team Exercise to uncover the vulnerabilities in the bank's perimeter/ internal network	Should the Red Team be performed in an assumed breach model as well or the entire activity should be performed in Blackbox approach	The initial Red Team activity focuses on uncovering vulnerabilities from the perimeter/ internal network perspective. The inclusion of an assumed breach model will be mutually agreed upon and defined with the successful bidder as part of the detailed Red Team mission objectives.
80	36	Section III - Scope of Work	Incident Response Readiness Assessment (Annual)	Can the Bank clarify if the Incident Response Readiness Assessment (IRRA) should cover all IT assets across DC, DR, NDR, and branch offices, or will a defined subset be provided?	IRRA should cover all IT assets including servers, databases, network devices, security appliances (Firewall, WAF, NIPS, Proxy, EDR, HIPS), endpoints, and business applications as per RFP Pages 36-37, Section III. Coverage includes DC, DR, NDR locations and sample branches. Assessment evaluates existing monitoring, logging, detection technologies, network architecture, and incident response capabilities across the bank's entire IT ecosystem.

81	37	Phase 1 - IRRA	Review of monitoring, logging, detection technologies, and IR plan	Will the Bank provide current incident response plans, SOPs, and security architecture documents for assessment, or is the bidder expected to create these from scratch?	Bank will provide existing IR documentation including current incident response plans, SOPs, CCMP (Cyber Crisis Management Plan), playbooks, and security architecture documents during Phase 1 engagement as per RFP Page 37, Point 1. Vendor will perform comprehensive gap assessment on existing cyber security incident handling procedures and various procedure documents to identify deficiencies.
82	36-37	Phase 1: Incident Response Readiness Assessment	Preparation & gap analysis for IR capability	Will the Bank provide existing IR documentation (IR Plan, SOPs, CCMP, playbooks) for gap assessment, or is the bidder expected to draft these entirely?	Bank will provide existing IR documentation including current incident response plans, SOPs, CCMP (Cyber Crisis Management Plan), playbooks, and security architecture documents during Phase 1 engagement as per RFP Page 37, Point 1. Vendor will perform comprehensive gap assessment on existing cyber security incident handling procedures and various procedure documents to identify deficiencies.
83	39	Phase 2: Incident Identification	Identification, categorization, 24/7 support, SLAs	What SIEM/SOC platforms, log sources, and threat intelligence feeds are currently in use, and will the Bank provide access to these	Current SIEM/SOC platforms, log sources, and threat intelligence feeds information will be shared during assessment phase as per RFP Pages 37-38. Vendor will evaluate existing security event

				for faster identification?	monitoring systems including DHCP logs, DNS logs, network traffic logs, event logs from endpoints/servers, logs from DLP, EDR, WAF, Firewall, HIPS, VPN, Active Directory, and provide recommendations for reconfiguration/upgrade.
84	39	Phase 2: Incident Identification	SLAs: 2-hour acknowledgement, 4-hour response	For on-site support, will the Bank facilitate access to restricted DC/DR/NDR/HO premises within SLA timelines, and provide required remote connectivity if travel delays occur?	Response timelines as per RFP Pages 38, 146-150: 24x7x365 support, acknowledge receipt within 2 hours, start IR within 4 hours. Onsite support: Tier-1 cities (12 hours), other cities (24 hours) excluding travel time. Resolution: Critical (2 days), High (4 days), Medium (7 days), Low (10 days). Penalties apply for delays.
85	39	Phase 2: Incident Identification	CERT-In empanelled auditor validation	Should every incident report be vetted by a CERT-In auditor, or only specific categories of major incidents (e.g., regulatory notifiable breaches)?	Every incident response and forensic investigation report must be duly vetted by CERT-In empanelled auditor as per RFP Page 38, Point 6. This requirement applies to all incidents to ensure reports are acceptable to Indian regulators. Only CERT-In empanelled service providers are eligible to bid (mandatory eligibility criteria as per RFP Page 30, Point 4).
86	39-40	Phase 3: Containment	Regulatory & stakeholder coordination	Will the vendor be responsible for direct liaison with regulators, LEAs, PR/Media, or will the Bank act as the primary point of	Bank will handle direct liaison with regulators, LEAs, PR/Media, and other external stakeholders as per RFP Page 39, Phase 3. Vendor shall assist in reporting and

				contact with vendor advisory support?	notification to regulatory and statutory authorities, Law Enforcement Agencies, Bank's Public Relations/Social Media Department, HR Department as required, but primary responsibility lies with the bank.
87	40	Phase 4: Analysis	Log retention and investigation scope	What is the Bank's current log retention period, and will vendors be allowed to recommend changes to retention/storage policies to support forensic analysis?	Current log retention details will be shared during engagement. Vendors are allowed to recommend changes to log retention policies based on assessment findings as per RFP Page 39, Phase 4, Point 1. Logs should be available for export in supported formats and not in proprietary formats for audit/compliance purposes. Minimum 3-year retention recommended for incident analysis.
88	40	Phase 4: Analysis	Investigation coverage	Does the scope of analysis extend to third-party hosted services such as cloud (O365, AWS, Azure), Fintech integrations, and outsourced IT providers?	Analysis scope extends to third-party hosted services including cloud platforms (O365, AWS, Azure), fintech partnerships, and other external services as per RFP Page 39, Phase 4, Point 2. Vendor should be able to perform investigation on different technologies and assets inclusive of all technologies, applications, devices available in Bank's IT-Ecosystem including cloud environments.

89	41	Phase 5: Eradication	Threat removal & vulnerability mitigation	Should the vendor also propose patching/configuration hardening, or will remediation be limited to advisory with the Bank's internal IT executing fixes?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
90	41	Phase 6: Recovery/ Monitoring	System restoration & monitoring for remanence	What is the expected monitoring duration post-incident (e.g., 7/15/30 days), and will this vary based on severity level of the incident?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
91	42	Phase 7: Reporting & Lessons Learned	Threat briefing, RCA, post-incident review	Does the Bank require executive-level summaries (CISO/CXO boards) distinct from technical RCA reports, and in what frequency (per incident vs quarterly)?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
92	61	Incident Response Timelines	Initial response within 4 hours	In case of remote Tier-2/3 locations, will the Bank facilitate remote access for initial containment before on-site presence?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
93	126	Broad Scope of Work	Tabletop Exercises (Annual)	Can the Bank confirm if Tabletop Exercises should involve only IT/SOC teams, or will they include cross-functional stakeholders such as Legal, PR, and Compliance?	Tabletop exercises are discussion-based activities covering scenarios like ransomware, data breach, DDoS attacks, malware incidents as per RFP Pages 144-145. Exercises validate incident response plans, test communication channels, assess decision-making

					under pressure. Must include various stakeholders and provide actionable recommendations for improvement.
94	145	Tabletop Exercise	Scenario-based assessments	Will the Bank define the tabletop scenarios (e.g., ransomware, DDoS, insider threat), or is the bidder expected to propose scenarios aligned to current threat landscape?	Tabletop exercises are discussion-based activities covering scenarios like ransomware, data breach, DDoS attacks, malware incidents as per RFP Pages 144-145. Exercises validate incident response plans, test communication channels, assess decision-making under pressure. Must include various stakeholders and provide actionable recommendations for improvement.
95	150	Incident Response SLA	Critical incident resolution within 2 days	How will the Bank define 'incident resolution'? Does it mean containment and recovery, or full eradication and RCA (Root Cause Analysis) completion?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
96	42	A	Forensic Readiness Assessment	How frequently does the Bank expect the forensic readiness assessment to be conducted, and what is the process for validating closure of identified gaps?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
97	42	A	Forensic Readiness Assessment	What are the specific triggers or criteria for initiating a digital forensic	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer

				investigation (e.g., type of incident, severity, regulatory requirement)?	to the clauses mentioned in the RFP for detailed clarification.
98	43	B	Evidence Collection & Chain of Custody	What are the Bank's protocols for maintaining chain of custody for digital evidence, especially for legal or regulatory proceedings?	All evidence must be legally admissible in Indian courts as per RFP Pages 44-46. Chain of custody maintenance mandatory throughout investigation. Vendor should provide legal evidence valid in courts and present same if required. Reports should be in formats acceptable to judiciary platforms and regulatory authorities. Professional testimony may be required.
99	43	B	Evidence Collection & Chain of Custody	Are there any mandated tools or platforms for evidence collection, imaging, and preservation, or can the vendor propose industry-standard solutions?	Vendor must arrange forensic tools at own cost as per RFP Page 38, Point 8. Tools should be commercially licensed, capable of handling different OS (Windows, Linux, Unix, Mac), databases, mobile devices, and cloud environments. Chain of custody maintenance mandatory. Tools must be approved by bank before deployment.
100	43	B	Evidence Collection & Chain of Custody	How should the vendor handle evidence that is stored in cloud environments or on third-party platforms, considering data localization requirements?	Analysis scope extends to third-party hosted services including cloud platforms (O365, AWS, Azure), fintech partnerships, and other external services as per RFP Page 39, Phase 4, Point 2. Vendor should be able to perform

					investigation on different technologies and assets inclusive of all technologies, applications, devices available in Bank's IT-Ecosystem including cloud environments.
101	43	C	Scope of Forensic Investigations	What types of incidents (e.g., data breach, insider threat, ransomware, fraud) will automatically trigger a full forensic investigation?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
102	43	C	Scope of Forensic Investigations	Are there any restrictions on the types of devices or systems (e.g., mobile, cloud, legacy) that can be examined during a forensic investigation?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
103	43	C	Scope of Forensic Investigations	Will the vendor be expected to perform live forensics on running systems, or only post-incident analysis?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
104	44	B	Collaboration with Internal Teams	How should the forensic team coordinate with internal IT, SOC, and legal/compliance teams during an investigation?	Coordination will be through Bank's identified SPOC.
105	44	B	Third-Party Involvement	Are there any special procedures for handling evidence involving third-party vendors, outsourced IT, or supply chain partners?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.

106	44	D	Reporting & Legal Admissibility	Is the vendor expected to provide expert testimony or support for regulatory/legal proceedings, and what is the engagement process?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
107	45	E	Training & Knowledge Transfer	What are the expectations for training Bank personnel in forensic readiness, evidence handling, and incident documentation?	Onsite training to minimum 10 designated bank personnel in first year as per RFP Page 43. Training covers digital forensic investigation, evidence preservation, chain of custody, legal requirements. Service provider shall conduct training to ensure proper documentation, procedures, policies during forensic investigation. Annual refresher training mandatory with practical exercises.
108	45	E	Training & Knowledge Transfer	How many staff members are to be trained, and what is the preferred mode (onsite, remote, workshops)?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
109	45	F	Tools, Technology, and Data Handling	Are there any restrictions on the use of proprietary vs. open-source forensic tools for investigations?	Vendor must arrange forensic tools at own cost as per RFP Page 38, Point 8. Tools should be commercially licensed, capable of handling different OS (Windows, Linux, Unix, Mac), databases, mobile devices, and cloud environments. Chain of custody maintenance mandatory. Tools must be approved by

					bank before deployment.
110	45	F	Tools, Technology, and Data Handling	What are the Bank's requirements for secure storage, retention, and eventual disposal of forensic data and evidence?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
111	46	G	Compliance & Regulatory Alignment	What is the process for updating forensic procedures and policies in response to regulatory changes or audit findings?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
112	6	SCHEDULE [A]	Last Date of Submission/ Closing Date in Online & Offline Mode	Please allow extension on bid submission of at least 4 weeks from date of publishing of query responses.	Extension provided till 28.10.2025. Refer GeM portal.
113	81		Minimum 5 years' experience in IR & forensics across at least 5 countries	Kindly confirm if client references from any industry vertical are acceptable, or BFSI references are mandatory or refrences from associated memener firmsPart of BDO India LLP) are acceptable.	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
114	81		Deep knowledge of APT attack methodologies, esp. Asia-India & global financial sector	Please clarify if supporting evidence (e.g., threat intel reports) must be submitted at bid stage.	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.

115	81		Release of ≥5 public reports/whitepapers on cybersecurity	Would internal (client-confidential) reports count if public release is not possible?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
116	82		Use of own tools/scripts + OS inbuilt tools for telemetry collection	Should bidders list all proprietary tools or only key categories?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
117	82		Tools must be commercially licensed with proper entitlement	Is documentary proof of license required with the bid or post-award?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
118	82		Tools must support telemetry collection from IT Networks/Systems/Endpoints	Any specific EDR/SIEM integrations expected?	Current SIEM/SOC platforms, log sources, and threat intelligence feeds information will be shared during assessment phase as per RFP Pages 37-38. Vendor will evaluate existing security event monitoring systems including DHCP logs, DNS logs, network traffic logs, event logs from endpoints/servers, logs from DLP, EDR, WAF, Firewall, HIPS, VPN, Active Directory, and provide recommendations for reconfiguration/upgrade.
119	82		Capability for malware analysis & reverse engineering	Is in-house capability mandatory or can it be subcontracted?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses

					mentioned in the RFP for detailed clarification.
120	82		Support across full DFIR lifecycle (triage to post-incident review)	Please confirm if ongoing retainer support is expected after recovery.	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
121	82		Maintain chain of custody and secure evidence disposal	Will the client provide a preferred evidence format or template?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
122	82		Maintain latest IOC and threat-intel library	Would subscription to a commercial threat-intel platform suffice?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
123	83		Experience engaging with global law enforcement/CERTs	Is a minimum number of engagements required for eligibility?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
124	83		Recognition in Forrester/Gartner/IDC etc. in last 3 years	Is recognition in any one report sufficient?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
125	83		Responded to >100 incidents in last 5 years, ≥10% DFIR in BFSI	Will redacted engagement summaries be acceptable as proof?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP

					for detailed clarification.
126	83		≥10,000 cumulative DFIR/Red Team hours in last 3 years	Is self-certification with customer countersign acceptable?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
127	83		More than 25 MITRE ATT&CK references	Kindly clarify evidence format for MITRE mapping.	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
128	83		Profiles of ≥10 APT/Threat Actor groups with insights	Is an internal threat-intel report acceptable as evidence?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
129	84		Endpoint agent/EDR used on ≥1 million endpoints globally	Will OEM attestation be required?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
130	84		Dedicated team of >100 security researchers/analysts/responders	Is global headcount acceptable or India-specific?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
131	84		Provide 3 client references with engagement details	Can names be redacted with NDA proof?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP

					for detailed clarification.
132	84		Provide DFIR case examples of APT intrusions in last 3 years	Should examples be global or India-specific?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
133	84		Provide DFIR case examples of ransomware attacks in last 3 years	Is a minimum of 3 cases required or more?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
134	84		Experience with malware analysis & tools used	Can third-party lab support be cited?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
135	85		Provide 5 sample team resumes (names not needed)	Is a standard skill-matrix acceptable instead of resumes?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
136	85		Experience presenting to Board-level bodies	Should we provide a presentation sample or only description?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
137	85		Provide 3 redacted final reports of DFIR/Red Team/Cyber Drill	Is a sanitized executive summary acceptable if full report cannot be shared?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP

					for detailed clarification.
138	85		3 evidences of forensic work legally admissible in court in last 5 years	Is a client confirmation letter sufficient?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
139	85		Team includes certified ethical hackers (OSCP/CREST etc.)	Are equivalent certifications (e.g., GPEN) acceptable?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
140	85		Scope of testing must be clearly defined and approved	Will client provide a scope template or should bidder propose?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
141	85		Attack simulation uses advanced tools/techniques	Are there any prohibited tools or frameworks?	All methodologies must comply with international standards (NIST, OWASP, PCI, PTES, OSSTMM) as per RFP requirements. Vendor must follow established frameworks for incident response, forensic investigation, red team exercises. All approaches subject to bank approval and regulatory compliance.
142	85		Testing must not disrupt critical operations	Is there a specific maintenance window requirement?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP

					for detailed clarification.
143	86		Detailed report of vulnerabilities & remediation	Should reporting format follow client template?	Key deliverables include assessment reports, gap analysis, remediation recommendations, training materials, incident reports as per respective service sections. Reports must be comprehensive with executive summaries suitable for board presentation. All reports in formats acceptable to regulators with proper documentation and evidence trail.
144	86		Testing scenarios customized to client environment	Will client provide threat landscape inputs?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
145	86		Secure collection and storage of logs/evidence	Should data be stored on-prem or bidder's secure cloud is acceptable?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
146	86		Confidentiality & NDAs mandatory	Will client share standard NDA template or bidder to propose?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
147	86		Follow-up remediation support if required	Should cost for follow-up be included in commercial bid?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses

					mentioned in the RFP for detailed clarification.
148	86		Facilitated, scenario-based tabletop exercises	How many exercises are expected annually?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
149	86		Scenarios tailored to client cyber risks	Will risk scenarios be provided by client or derived by bidder?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
150	86		Clear objectives/outcomes established	Will objectives be finalized during kickoff workshop?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
151	86		Pre-defined environment for real-time decision making	Will client provide environment or should bidder simulate?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
152	86		Document lessons learned and improvements	Should final report follow a specific template?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
153	86		Post-exercise debrief report	What is the expected turnaround time for report submission?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP

					for detailed clarification.
154	87		Simulate comprehensive attacks across networks/apps/endpoints	Are any specific technology stacks to be included?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
155	87		Include multiple attack vectors (malware, phishing, social engineering etc.)	Are insider threat scenarios required as well?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
156	87		Assess effectiveness of detection/response/recovery	Will client share existing IR metrics for baseline?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
157	87		Use simulated threat-intel feeds & attack techniques	Should bidder provide threat-intel subscription as part of scope?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
158	87		Provide comprehensive post-drill report with gaps & recommendations	Is a management summary plus technical appendix acceptable?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
159	36		Scope of work	The scope mentioed in RFP can you specify the location where this activity will be performed	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP

					for detailed clarification.
160	59		Penalty Clause	Can you provide some relaxation on the penalty clause	Performance measured through SLAs with specific penalties as per RFP Pages 146-150: Rs. 5,000-25,000 per day for service delays, Rs. 10,000 per hour for response delays. Maximum penalty 10% of contract value. Penalties apply for missed timelines in deliverables, response times, and resolution targets.
161	37		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.	Can you provide some relaxation on the penalty clause	Performance measured through SLAs with specific penalties as per RFP Pages 146-150: Rs. 5,000-25,000 per day for service delays, Rs. 10,000 per hour for response delays. Maximum penalty 10% of contract value. Penalties apply for missed timelines in deliverables, response times, and resolution targets.

162	41		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.	Will this be like purple teaming activity where we will be creating rules/signatures for any identified vulnerabilities in previous assessments or as and when a threat is identified (DFIR)	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
163	41		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.	What if the tool cannot be installed and that becomes a limitation while gathering/analyzing logs	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
164	147	4: Payment terms	Payment will be made yearly in arrears, after completion (on acceptance by Bank) of services.	Request you to make it yearly advance basis as this is the services component for us	Adhere to terms and conditions of the RFP
165	General	Services delivery	Services like IRRA, Cyber Drill, Foresics, Red Teaming services to be delivered onsite	Request you to allow the Model of delivery of services in Hybrid model , So that we can leverage global skills capability as well.	Adhere to terms and conditions of the RFP
166	59	SLA Penalty	Penalty of Rs.25000 Per Day will be applicable, in case of delay.	Request to make a maximum cap with 5% for that monthly Invoice value of activity	Adhere to terms and conditions of the RFP

167	33	8.4	Hours estimation	How many hours should we include in a "man-day"?	8 Hours = man-day
168	42	A	Compliance with Bank's Cyber Crisis Management Plan	Will the bank provide the CCMP under NDA to aid in estimation of the effort required?	Will be shared with the successful bidder
169	42	A	Compliance with RBI Information Security guidelines & Cert-In guidelines	Will the bank specify the guidelines they wish to be assessed against to aid in estimation of the effort required?	Adhere to terms and conditions of the RFP
170	42	A	Compliance with any other legal requirements.	Will the bank provide a legal opinion of the legal requirements or should this be factored into the bidder's costs?	Adhere to terms and conditions of the RFP
171	45	B	Ability and experience in providing IT Forensic and e-Discovery services to harvest data from IT security devices.	Does the reference to eDiscovery on page 45 relate only to the collection of data?	Yes

172	42	A	RBI Information Security guidelines, Cert-In guidelines, any other legal requirements	What the other leagal requirements covers?	Legal requirements with respect to Cyber/Digital Forensics
173	42	A	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	What industry standards and Government regulations to be treated as a benchmark?	Indian standards for Cyber/Digital Forensics, Government regulations in India(IT act, RBI, CERT-In, NCIIPC, SEBI framework/guidelines etc.)
174	43	A	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.	What are the specific Cert-In, RBI, NCIIPC guidelines that needs to be considered?	Adhere to terms and conditions of the RFP
175	43	A	Assisting with identification of High Value Targets (HVTs) and weaknesses based on common methodologies. HVTs could be People, Systems, Processes or Technology	Are the HVTs are defined? Does Indian Bank share the lists of HVTs?	This requirement is addressed as per the relevant RFP sections and industry best practices. Please refer to the clauses mentioned in the RFP for detailed clarification.
176	46	B	Normal operations are affected for a very limited period of time, if at all (limited interference of the crime scene on normal life).	Need more clarity on the timelines.	During forensic investigation normal operations should not be impacted for long period of time

177	57	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	Whether these timelines are rigid or depend on mutual agreement depending on the nature of the incident?	Adhere to terms and conditions of the RFP
178		10	IR support vendor shall submit comprehensive incident report within 24 hours from incident resolution & restoration to Bank	Usually, a priliminary report can be provided with in 24 hours. Will there be an additional time provided for comprehensive report?	Adhere to terms and conditions of the RFP

GeM Bid Ref: GEM/2025/B/6707442 **Date:** ***15.10.2025***

ANNEXURE-XXI

Undertaking that Bidder or its Subsidiaries are not engaged with Indian Bank for Incident Services, Forensic Services and Security Solution implementation in the last TWO years.

The Asst. General Manager

Indian Bank

Information System Security Department,

3rd Floor 66, Rajaji Salai, Chennai – 600 001

Dear Sir,

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

We M/s_____, a company incorporated under the Companies Act, 1956 OR Companies Act, 2013 OR Partnership Bidder registered under LLP Act, 2008 with its headquarters at,

_____ do hereby confirm that we and any of our subsidiary have not been engaged with Indian Bank for any of the following services in the last TWO years:

a. Incident Response Services.
b. Forensic Services
c. Security Solutions Implementation.

This declaration is being submitted and limited to, in response to the tender reference mentioned in this document.

Thanking You,

Yours faithfully,

Date: _____
Place: _____

Signature of Authorized Signatory

Name:
Designation:
Seal: