CENTRALISED PROCUREMENT & PARTNERSHIP DIVISION HO, 5, Sansad Marg, New Delhi – 110 001

Finalized response to Pre-Bid queries and corrigendum for RFP for Engaging Services of Incident Response Retainer (IRR).

Sr. No.	RFP Page No.	RFP Clause Name & No.	RFP Clause	Bidder's Query/ Suggestion/ Remarks	RESPONSE
1	58	Annexure 2 -Eligibility Criteria & Pt no. 4	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 as on last date of bid submission.	Bidder can use OEM experience in this	Please be guided as per the RFP and its subsequent corrigenda.
2	59	Annexure 2 -Eligibility Criteria & Pt no. 5	The bidder must be Cert-in empanelled.	If Bidder is not an Cert-in Empanelled and OEM is so Bidder can use that	Please be guided as per the RFP and its subsequent corrigenda.
3	NA	General Query	GEM/2025/B/6283066	Please provide some extension to submit the bid.	Please check GeM portal at regular intervals for any update in this matter.
4	NA	General Query	GEM/2025/B/6283066	Please clarify how unused hours at the end of retainership period shall be used.	Successful bidder will not be paid for unused hours.
5	41	3.1 Scope of Work	The maximum time man-hours for incident response readiness assessment (IRRA) are 80 hours.	We understand that log retention review, cyber incident response policy review and other activities as part of cyber incident response readiness assessment shall take more than 80 hours, we request you to update time for the IRR assessment to 200 hrs. Further, we wanted to confirm if we consume over the prescribed hours (80) for IRRA activity, would we be able to invoice for additional effort spent.	Please be guided as per the RFP and its subsequent corrigenda.

6	41	3.1 Scope of Work	for This phase will Improve PNBs Incident & Forensic response plan and procedures. In this phase vendor will help the Bank to establish /implement/review an incident response plan and forensic readiness capability so that Bank is ready to respond to it. Under this preparation phase, which involves preparing for potential cyber incidents by establishing incident & forensic response plans, identifying the procedural and technical gaps in existing IT Setup w.r.t. incident & forensic response readiness, creating an incident /forensic response team representative from Bank and IRR vendor personals, defining roles and responsibilities, and implementing monitoring and detection systems. Workshops /assessment to be conducted with various stakeholders in the Bank in order to understand Bank environment to enable to Bidders Incident response team to respond, mitigate, recover from attacks asap. This phase is to review banks existing Incident response plans, technologies deployed, log Sources in place to detect/analyses to be checked and readiness in order to respond to attacks/ breaches within stipulated timelines. The maximum time man-hours incident response readiness assessment (IRRA) are 80 hours.	Please specify all security/monitoring solutions that are deployed in the present environment.	Please be guided as per the RFP and its subsequent corrigenda. PNB adheres to RBI CSF 2016 and as such, necessary security measures are adhered to via necessary solutions and processes. Further details will be shared with successful bidder as per requirement.

7	41	3.1 Scope of Work	The successful bidder should perform the gap assessment on existing policies, procedures and SOPs of Cyber Security incident handling/ Cyber crisis management plan and various other procedure documents.	Please clarify if an existing CCMP is in place?	Please be guided as per RFP. PNB adheres to RBI CSF 2016 and as such, necessary security measures are adhered to via necessary solutions and processes. Further details will be shared with successful bidder as per requirement.
8	41	3.1 Scope of Work	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; 1. Centralized deployment/execution of IOC scanners or other tools designed to obtain digital evidence. 2. Credentials management (e.g. password change policies) 3. System backup architecture and backup recovery. 4. Logging security event sources 5. Log sources / security controls check. 6. Creation of SOPs for addressing incidence.	For security event logging, are there any existing system (SIEM, EDR) are deployed in the environment. Please clarify.	Please be guided as per the RFP and its subsequent corrigenda. PNB adheres to RBI CSF 2016 and as such, necessary security measures are adhered to via necessary solutions and processes. Further details will be shared with successful bidder as per requirement.
9	42	3.1 Scope of Work	Phase 1: Incident Response Readiness Assessment (IRRA).	Please clarify the frequency of the Incident Response Readiness Assessment. Do we have to perform this annually or once in 3 years?	Once

10	43	3.1 Scope of Work	The vendor will setup the dedicated IT infrastructure for PNB 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 IRR analysts, during incident response for log analysis and correlation. No logs or metadata should be transferred outside of India. The cloud instance should be preserved at least for 3 years of end of contract or based on agreed retention period as per Bank written confirmation.	Please clarify if evidence can be preserved in encrypted hard drives.	Evidence needs to be stored on dedicated forensic workstation/ dedicated IRT infrastructure within India. The system for the evidence needs to be mandatorily encrypted with keys provided to the Bank and necessary Chain-of-custody needs to be preserved furring the entire incident lifecycle and beyond.
11	43	3.1 Scope of Work	During Incident response readiness review exercise the vendor should clearly define below modalities in detail. • Incident Response Retainer team structure and responsibilities • Communication between different teams (IRR, CISD and other stakeholders from Bank) will took 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 IRR Playbooks for the Bank.	Please Clarify the frequency for updating the IRR playbooks for the bank.	Update of IRR playbook needs to be done once post the IRRA and then after lessons learned stage of any incident reported
12	43	3.1 Scope of Work	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, and • Assist in clearing/signoff of Comprehensive security review (CSR) of such tools, devices, and technologies before completion of Phase 1 (IRRA)	Deployment of any security solution/tool will depend on the type of cyber incident; the choice of tool shall be decided on the basis of each security incident. The tool will be installed upon confirmation from PNB.	Necessary tools shall be installed after mutual discussion as per requirement.

13	43	3.1 Scope of Work	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 analysing data from various sources, such as intrusion detection systems, log files, applications, devices and network traffic etc.	Please clarify if there is defined categorization for the bank or this categorization shall also be defined by the bidder.	Categorization of the cyber security incident needs to be derived from the Bank's defined standards and procedures, which will be shared with successful bidder as per need.
14	43	3.1 Scope of Work	The Service provider should 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. The IR analyst should be at onsite location of breach, if required, as per timelines mentioned in Timelines and delivery schedule table point no 4. &5 'Incident response and resolution timelines.	Please specify the locations where KPMG team need to visit in case of an incident.	The onsite team needs to visit bank's locations. such as, PNB Head Office, administrative offices, branches, and foreign centres.
15	44	3.1 Scope of Work	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.	Please clarify the expectations from the bidder.	Logs collected should be available in formats as specified by the Bank and should not be proprietary to a specific solution
16	45	3.1 Scope of Work	Bidder shall review the incident/forensic response plan and policies as and when required by Bank.	Please clarify the frequency for reviewing Incident Response Plan for the bank.	Please be guided as per the RFP and its subsequent corrigenda.
17	45	3.1 Scope of Work	Bidder shall establish an incident/forensic response plan for ransomware attack, review and update the same as per industry standard.	Please clarify if there is an existing IR plan in place for ransomware.	Please be guided as per the RFP and its subsequent corrigenda.
18	45	3.1 Scope of Work	Bidder shall conduct trainings of Bank personnels to ensure proper documentation, procedure, policies during a forensic investigation.	Please clarify the frequency for trainings needed to be conducted.	initial training once. Subsequentially after lessons learned phase post every incident

19	45	3.1 Scope of Work	Bidder shall determine where critical data is stored and how it can be accessed during forensic investigation.	Please clarify if KPMG needs to build and implement the policies for the critical data storage.	Bidders need to review the same during IRRA and act accordingly
20	45	3.1 Scope of Work	Bidder shall assist in preparing the advisory for Bank employees and customer.	Please clarify the frequency for which advisories need to be shared	Quarterly
21	46	3.1 Scope of Work	Bidder shall provide maintenance support for Hardware/ Software/ Operating System/ Middleware over the entire period of Contract.	Please clarify this clause and what is expected from the bidder? We shall provide support from OEM's for the deployed products by KPMG, if any.	Bidder needs to provide OEM support for any solution/ tool deployed or used for IRR activity during the entire course of the contract
22	46	3.1 Scope of Work	Bidder shall provide the Keys to decrypt the data in case of ransomware and others attack.	Please clarify this clause. We request that this clause shall be removed/updated to reflect that decryption keys may not always be available during a ransomware attack.	Please be guided as per the RFP and its subsequent corrigenda.
23	46	3.1 Scope of Work	All software, hardware, storage, etc. should be included under the L1 bidding cost, no additional cost will be provided.	Please clarify if KPMG needs to bear the cost of all other devices recommended during the engagement.	Please be guided as per the RFP and its subsequent corrigenda.
24	47	3.2 Training	Bidder has to arrange for providing advance hands-on in-premises training to the Bank officials for day-to-day troubleshooting, configuration, customization and maintenance of proposed IRR Services before Go-Live as a part of project implementation without any additional cost to the Bank.	Please specify the frequency of trainings	Initial training once. Subsequentially after lessons learned phase post every incident

25	47	3.2 Training	Further, post implementation bidder has to arrange similar advanced hands-on training (in-premises) including troubleshooting, configuration, customization etc. half yearly to 10 officials of the Bank (in 2 batches having 5 officials each) each to enable Bank resource to deploy (administrative users) and operate (end users) the IRR services efficiently as well as troubleshooting and administration of the deployed services.	Please specify the locations where KPMG team need to provide the training	At PNB HO in Delhi NCR
26	52	3.8 Other terms and conditions	Location of Onsite technical support person can be changed as per the Bank requirement. It may be DC, NDC and DR and any other site of the Bank.	Please specify the locations of DC and DR	Delhi-NCR (DC), Mumbai Metropolitan area (DR)
27	44	3.1 Scope of Work	Phase 4 - Analysis: This phase will involve analysing 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.	Please clarify if we need to provide forensic imaging service in case of a cyber incident? Please clarify if KPMG will bear the cost of hard drives or other hardware requirement for forensic imaging?	Please be guided as per the RFP and its subsequent corrigenda.
28	44	3.1 Scope of Work	The vendor should restore the attacked system/ operations to normal state and should ensure that the systems are functioning normally and remediate vulnerabilities to prevent similar incidents.	Please clarify if KPMG team needs to guide IT team to restore the systems and IT network in case of cyber incident or do we need to provide full restoration services?	Please be guided as per the RFP and its subsequent corrigenda.
29	49	3.4 Timelines and delivery schedule	Incident Response services initiation timelines: Outside India- Overseas offices and branches: 48 hours	Please clarify the geographical scope of this assessment. Does it include all branches, or its limited to specific locations. Request you to share the number of countries in which Incident Response Retainer contract will be active. Deployment of resources shall be subject to VISA availability.	Please be guided as per the RFP and its subsequent corrigenda. The scope includes any of the PNB Head Office, administrative offices, branches, and foreign centres. The scope is not static as the count of offices and branches gets updated frequently. Bidder may check

					www.pnbindia.infor further detail.
30	93	Annexure 16	Service provider must have in-house capabilities or experience to engage with law enforcement agencies and CERTs of different countries to aid in investigations. Public reference on case studies of engagement with law enforcement agencies shall be provided.	In IR engagements client name were not disclosed publicly. We have communication with the CERT over emails.	Masked details will suffice
31	95	Annexure 16	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.	Deployment of any security solution/tool will depend on the type of cyber incident; the choice of tool shall be decided on the basis of each security incident. The tool will be installed upon confirmation from PNB.	Please be guided as per the RFP and its subsequent corrigenda.
32	44	3.1 Scope of Work	Phase 6 Recovery/Monitoring: In this phase, the incident response team works to restore normal business operations and ensure that all systems are functioning properly. This shall also involve conducting user awareness training, updating policies and procedures, and reviewing incident response plans. 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.	Please clarify that are we required to conduct 24*7 monitoring of the network for specific period of time agreed between PNB and KPMG in case of a cyber incident or only threat hunting activity is required?	Please be guided as per the RFP and its subsequent corrigenda.
33	48	3.4 Timelines and delivery schedule	IRR shall submit comprehensive incident report within 24 hours from incident resolution & restoration to Bank.	We will provide regular updates depending upon the complexity of the cyber incident. Status deck will be presented for daily updates. Final report will be shared post completion of cyber incident analysis.	Please be guided as per the RFP and its subsequent corrigenda.
34	50	3.5.1 Penalty Terms	Penalty Terms	We kindly request the PNB team to consider providing some flexibility	Please be guided as per the RFP and its subsequent corrigenda.

				regarding the penalty terms depending upon the type of cyber security incident.	
35	33	1.13.34 Limitation of Liability	Vendor's aggregate liability under the Agreement shall be limited to a maximum of the Agreement value. For the purposes of this clause, Agreement value at any given point of time, means the aggregate value of the purchase orders, paid by Bank to the Vendor that gives rise to claim, under this Agreement.	This clause shall not apply to any law, judicial/ quasi-judicial determination or Government's directions to the contrary, and to the maximum extent permitted by law, the Vendor shall be liable to Bank for any consequential/ incidental, or indirect damages arising out of this agreement	Please be guided as per the RFP and its subsequent corrigenda.
36	41	3.1 Scope of Work	Bidder shall assist regulatory bodies during their forensics investigation, if required	We request you to include the following disclaimer: "Any product of services shall be for the internal use of the Client and shall not be disclosed to any third party without prior written consent of KPMG Assurance and Consulting Services LLP. Client shall not quote KPMG Assurance and Consulting Services LLP's name or reproduce KPMG Assurance and Consulting Services LLP's logo in any form or medium without KPMG Assurance and Consulting Services LLP's prior written consent."	Please be guided as per the RFP and its subsequent corrigenda.
37	23	1.13.17 Conflict of Interest	A bidder shall not have conflict of interest with other bidders. Such conflict of interest can lead to anti-competitive practices to the detriment of Bank's interests. The bidder found to have a conflict of interest shall be disqualified.	Please clarify ift the requirements of this entire clause shall be restricted to the engagement team members only	Please be guided by the RFP and its subsequent corrigendum.

38	24	1.13.23 Audit	All records with respect to any matters covered under this RFP/SLA shall be made available to auditors and or inspecting officials of the Bank and/or Reserve Bank of India and/or any regulatory authority and/or any statutory authority, at any time during normal business hours, as often as the Bank deems necessary, to audit, examine, and make excerpts or transcripts of all relevant data. The said records are subject to examination.	We request you to include the following clause : "Any audit shall be subject to the following: (i) the audit shall be restricted to the engagement and shall be conducted with prior reasonable notice (ii) The Bank or its authorized representatives shall execute a Non-Disclosure Agreement before such audit which shall govern the conduct of the audit and any results thereof; (iii) the auditors or the representatives of the Bank for the audit shall not be the Successful Bidder's competitors; (iv) the audit shall not be conducted more than once in a calendar year and twice in entirety; and (v) any findings during the audit, shall be shared with the Successful Bidder and be discussed and agreed mutually between the Bank and the Successful Bidder for its closure."	Please be guided by the RFP and its subsequent corrigendum.

39	82	Annexure 11	The Recipient shall, upon the request of the Disclosing Party, in writing, return to the Disclosing Party all drawings, documents and other tangible manifestations of Proprietary and Confidential Information received by the Recipient pursuant to this Agreement (and all copies and reproductions thereof) within a reasonable period. Each party agrees that in the event it is not inclined to proceed further with the engagement, business discussions and negotiations, or in the event of termination of this Agreement, the Recipient party will promptly return to the other party or with the consent of the other party, destroy the Proprietary and Confidential Information of the other party.	We request you to include the following clause: "We shall be allowed to retain sufficient documentation as part of our professional records to support and evidence the work performed by us. Such retention shall be subject to obligations of confidentiality mentioned herein."	Please be guided as per the RFP and its subsequent corrigenda.
40	10	1.5 Performance Bank Guarantee	The Performance Bank Guarantee shall act as a security deposit and either in case the Successful bidder is unable to start the project within the stipulated time or start of the project is delayed inordinately beyond the acceptable levels, the Bank reserves the right to forfeit the same.	Request this clause to be amended to consider the situations where the delay is not to be attributed to the bidder.	Any delay on part of bank will not be considered for invocation of Performance Bank Guarantee.
41	11	1.6 Bid Earnest Money	Bidder has to submit the Bid Earnest Money (EMD) of Rs.1,30,000 (Rupees One Lakhs and Thirty Thousand only),	If the NEFT is permissible instead of BG then please confirm if the given bank details will be same for the NEFT transaction?	Yes
42	11	1.6 Bid Earnest Money	Bidder has to submit the Bid Earnest Money (EMD) of Rs.1,30,000 (Rupees One Lakhs and Thirty Thousand only),	If the Bank Guarantee is transferred via NEFT, is Annexure 10 still required as supporting documentation?	No

43	27	1.13.28 Confidential Information	That if the vendor hires another person to assist it in the performance of its obligations under the Contract or assigns any portion of its rights or delegates any portion of its responsibilities or obligations under the Contract to another person, it shall cause its assignee or delegate to be bound to retain the confidentiality of the confidential information in the same manner as the Vendor is bound to maintain the confidentiality. This clause will remain valid even after the termination or expiry of this agreement.	Request to remove last line "This clause will remain valid even after the termination or expiry of this agreement."	Please be guided as per the RFP and its subsequent corrigenda.
44	29	1.13.29 Non-Disclosure Agreement	Even if any employee of the vendor leaves the job or his services are terminated/expires, the vendor shall ensure that Banks confidential information is not shared with any third party nor Banks confidential information is used to derive unauthorized profits out of it. Vendor shall continue to be responsible for any such act of its ex-employee and agrees to indemnify the Bank against any loss suffered by Bank due to disclosure of confidential information in such circumstances.	Request to remove this clause	Please be guided as per the RFP and its subsequent corrigenda.
45	33	1.13.34 Limitation of Liability	Vendor's aggregate liability under the Agreement shall be limited to a maximum of the Agreement value. For the purposes of this clause, Agreement value at any given point of time, means the aggregate value of the purchase orders, paid by Bank to the Vendor that gives rise to claim, under this Agreement. In the following circumstances limitation of liability shall not apply and the Vendor shall be liable for amount of cost, damages, compensation, penalty etc. suffered by the Bank: -	Request to remove line 'the Vendor shall be liable for amount of cost, damages, compensation, penalty etc. suffered by the Bank:	Please be guided as per the RFP and its subsequent corrigenda.
46	33	1.13.34 Limitation of Liability	5. Liability of the Vendor in case of fraudulent acts or wilful misrepresentation attributable to the Vendor regarding' the services provided under this Agreement. 6. Breach of the confidentiality.	Request to remove all these points	Please be guided as per the RFP and its subsequent corrigenda.

			7. Employment liabilities for vendor's staff relating to the period of their employment within contractual period while working with Bank. 8. Any liability/penalty/cost/compensation/charges etc. that cannot be capped or is excluded as a matter of applicable laws and imposed by the statutory authority/ government bodies/ court/tribunals etc. in relation to this Agreement, owing to the fault of the Vendor. 9. Any other breach caused due to the non-performance of the obligations of the Vendor under the Agreement. This clause shall not apply to any law, judicial/ quasi-judicial determination or Government's directions to the contrary, and to the maximum extent permitted by law, the Vendor shall be liable to Bank for any consequential/ incidental, or indirect damages arising out of this agreement.		
47	41	3.1 (1) Scope of Work	**Phase 1: Incident Response Readiness Assessment (IRRA).** This phase will Improve PNBs Incident & Forensic response plan and procedures. In this phase vendor will help the Bank to establish/implement/review an incident response plan and forensic readiness capability so that Bank is ready to respond to it. Under this preparation phase, which involves preparing for potential cyber incidents by establishing incident & forensic response plans, identifying the procedural and technical gaps in existing IT Setup w.r.t. incident & forensic response readiness, creating an incident/forensic response team representatives from Bank and IRR vendor personals, defining roles and responsibilities, and implementing monitoring and detection systems.	Is the service provider expected to implement any monitoring and detecting solution for PNB? Or is the requirement limited to readiness assessment of solutions that have already been implemented in the PNB environment? If implementation is required, would PNB like the bidder to support with project management and governance only or the implementation also, please clarify.	No implementation required or expected during IRRA phase.

48	41	3.1 Scope of Work	The maximum time man-hours for incident response readiness assessment (IRRA) are 80 hours	The given 80 man hours provided for IRRA services would be insufficient for the defined scope of work considering the complexity and enormity of the activities. The following activities would require reasonable hours: ----Establishing incident & forensic response plans ----Procedural and technical gaps in existing IT Setup ----Implementing monitoring and detection systems(Need clarity on this please refer to the Query NO: 08) ----Review banks existing Incident response plans ----Review technologies deployed ----Review Log sources ----Provide recommendations on how to reconfigure or upgrade existing security event monitoring ----Setup the dedicated IT infrastructure for PNB within India, either physical or in cloud instance ----Establish a process, and deploy/install necessary hardware, software, sensors, scripts, agents for collection of evidence for incident analysis, and Assist in clearing/signoff of Comprehensive security review (CSR) of such tools, devices, and technologies ----Recommendations on how to reconfigure or upgrade existing security	Please be guided as per the RFP and its subsequent corrigenda.

				event monitoring systems, backup solutions, security devices, etc. ----Gap assessment on existing policies, procedures and SOPs of Cyber Security incident handling/ Cyber crisis management plan and various other procedure documents. All the above mentioned activities are time consuming... for instance, the activities listed above regarding analysing gaps, logs and developing incident response plan may take significant time and effort, especially considering the size of PNB infrastructure including potentially large number of servers and network devices involved. Given a cap of 80 hours on the time assigned for IRRA covering the above-mentioned activities, it seems potentially challenging to cover them in detail. It is therefore requested that the man-hour allocation for IRRA shall be increased to a reasonable figure considering the size of PNB infrastructure.	

49	43	3.1(1.5) Scope of Work	The vendor will setup the dedicated IT infrastructure for PNB 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 IRR analysts, during incident response for log analysis and correlation. No logs or metadata should be transferred outside of India. The cloud instance should be preserved at least for 3 years of end of contract or based on agreed retention period as per Bank written confirmation.	What is the expected baseline for the processing, storage, network speed, rack space availability at PNB (in case of deployment of physical infra at PNB) and log retention period required for the log analysis tool? Will PNB provide adequate space with power backup for hosting the computer system for log analysis? Would the secure network connectivity to this computer system for remote access be provisioned by PNB?	The system does not necessarily need to be hosted at PNB Site but should be dedicated to PNB and be situated within India.
50	43	3.1 (2.4) Scope of Work	Bidder 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.	If the bidder is CERT-In empanelled, can the bidder vet the report themselves instead of going to 3rd party vendors/ Auditors?	The team documenting and analysing the report needs to be distinct from the team vetting the report. Both teams may belong to the same entity and be certified by Cert-In.
51	43	1.1 (1.8) Scope of Work	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, and · Assist in clearing/signoff of Comprehensive security review (CSR) of such tools, devices, and technologies before completion of Phase 1 (IRRA)	Is the requirement limited to readiness assessment of solutions that have already been implemented in the PNB environment OR does it require implementation of new solutions in the PNB environment? If Implementation is desired, then please suggest responses to the following queries: 1. The deployment of any security solution or tool will depend on the nature of the cyber incident. The selection of the appropriate tool will be determined based on the specific requirements of each incident.	No new deployment is required unless for the incident forensics activity. However, the list of the solutions to be used for this activity need to be shared with PNB well in advance.

				2. Please suggest whether the bidder can use the tools registered in him name for providing services to PNB? 3. Please also refer query no 16 in this context.	
52	43	3.1(1.9) Scope of Work	The vendor will provide recommendations on how to reconfigure or upgrade existing security event monitoring.	This requirement relates to review of SOC which would be a separate activity and require greater efforts exceeding 80 hours allocated to IRRA. Please suggest if this is required to be performed	Please be guided as per the RFP and its subsequent corrigenda.
53	44	3.1 (4.2) Scope of Work	The vendor should restore the attacked system/ operations to normal state and should ensure that the systems are functioning normally and remediate vulnerabilities to prevent similar incidents.	Please clarify if the bidder is only expected to assist in the restoration process which would mainly be done by the bank. Considering the criticality of the data residing in the banking environment (Software and hardware) it would be vital that handling of such asset would be done by the Administrator of those assets who would be familiar to the structure of the data and the interconnected architecture of the systems in the PNB environment; the role of the vendor would be to assist the administrator by way of recommendations or suggestions.	Please be guided as per the RFP and its subsequent corrigenda.

54	44	3.1 Phase 6 Scope of Work	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.	Are all the network devices integrated with SIEM? if yes, would the SIEM solution in use be extended to the bidder for investigation?	Applicable network devices are integrated with the Bank's SIEM. The SIEM solution will not be extended to the bidder. The bidder may however request specific logs pertaining to the incident to only complement the analysis.
55	46	3.1 (8.17, 8.21) Scope of Work	Bidder shall use/provide legally valid Software/ hardware/ firmware Solution. The detailed information on license count and type of license shall also be provided to Bank. All software, hardware, storage, etc. should be included under the L1 bidding cost, no additional cost will be provided	1. Details of software's and hardware required may please be provided as it will provide uniformity at arriving at the cost. 2. Under whose name would the tools be procured? 3. Is it permissible to use Opensource tool for providing the services?	1. PNB adheres to RBI CSF 2016 and as such, necessary security measures are adhered to via necessary solutions and processes. 2. The tools for the forensics activity should be in the name of the bidder. 3. Open-Source tools may be/may not be permitted subject to approval from bank's competent authority.
56	46	3.1 (4.3, 8.20) Scope of Work	The vendor should be able to perform investigation on different technologies, assets inclusive of all technologies, applications, devices residing in Bank's IT Ecosystem and the various resources required during the investigation should be scalable. Incident response and forensic response support should not be vendor specific; all software/OS/ Hardware /legacy systems should be under the scope of RFP.	What technologies/applications/ devices used in the bank are expected to be covered under the investigations?	Please be guided as per the RFP and its subsequent corrigenda. PNB adheres to RBI CSF 2016 and as such, necessary security measures are adhered to via necessary solutions and processes
57	46	3.1 (8.15) Scope of Work	Bidder shall provide maintenance support for Hardware/ Software/ Operating System/ Middleware over the entire period of Contract.	We understand that this would be limited to the Hardware /Software/OS/ Middleware supplied by the bidder during	Yes

				the course of this engagement. Please suggest further.	
58	46	3.1 (8.16) Scope of Work	All product updates, upgrades & patches shall be provided by the Bidder/ Service Provider free of cost during warranty and AMC/ ATS/ S&S period.	We understand that this would be limited to the Hardware/Software/OS/ Middleware supplied by the bidder during the course of this engagement. Please suggest further.	Yes
59	46	3.1 (8.18) Scope of Work	Bidder shall provide the Keys to decrypt the data in case of ransomware and others attack.	Given that decryption keys for many new ransomware variants may not be available it is requested that the Clause be altered to allow the recovery of the keys on best effort basis.	If available, then share, otherwise best effort basis.
60	47	3.2 (a) Training	Bidder has to arrange for providing advance hands-on in-premises training to the Bank officials for day-to-day troubleshooting, configuration, customization and maintenance of proposed IRR Services before Go-Live as a part of project implementation without any additional cost to the Bank	Please specify the frequency of trainings	Initial training once. Subsequentially after lessons learned phase post every incident
61	47	3.2 (b) Training	Further, post implementation bidder has to arrange similar advanced hands-on training (in-premises) including troubleshooting, configuration, customization etc. half yearly to 10 officials of the Bank (in 2 batches having 5 officials each) each to enable Bank resource to deploy (administrative users) and operate (end users) the IRR services efficiently as well as troubleshooting and administration of the deployed services.	Please specify the locations where the team is required to conduct the training sessions.	PNB HO at Delhi NCR
62	48	3.5 Terms of Payment	Penalties / liquidated damages, if any, shall be deducted from the invoice value	It is requested to specify the minimum and maximum percentage and that any penalties/ liquidated damages deducted shall only be for reasons that are solely and directly attributable to the Bidder	Please be guided as per the RFP and its subsequent corrigenda.

63	48	3.4 (3.3) Timelines and delivery schedule	Outside India- Overseas offices and branches -> 48 hrs.	Please suggest which overseas locations are expected to be covered and would initial remote support be allowed? It is requested that information in this regard will be helpful in making arrangements with our counterparts in those countries.	Please be guided as per the RFP and its subsequent corrigenda. The scope includes any of the PNB Head Office, administrative offices, branches, and foreign centres. The scope is not static as the count of offices and branches gets updated frequently. Bidder may check www.pnbindia.infor further detail.
64	53	3.10.3 Shortlisting of bidders Technical Evaluation	The bidder is deemed to be qualified if a minimum of 70% marks are achieved in the technical assessment criteria as per Annexure 17 (B). All the bidders who meet these criteria are deemed to be qualified, and the bidder with the lowest cost would be awarded the contract.	Annexure 17 (A) and Annexure 17 (B) are not given in the RFP. Request to please rectify the given clause	Please read Annexure 17(A) & Annexure 17(B) as Annexure 17
65	58	Annexure 2 – Eligibility Criteria	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 – 5 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.	Request to change 'AND' to 'OR' as the clients in general does not provide the Performance Certificate.	Please be guided as per the RFP and its subsequent corrigenda.

66	59	Annexure 2 – Eligibility Criteria	The incident responders should be holding at least any two of the following professional certifications or their Indian equivalent (as per Bank's discretion): (15 marks for any two certifications and thereafter additional 1 mark for each additional certification within maximum limit.) •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)	It is requested to also consider the degree holders in Cyber Security /Forensic field	Please be guided as per the RFP and its subsequent corrigenda.
67	93	Annexure 16 Pn (1) Technical Functional Specification Compliance for Incident Response Retainer (IRR) Services.	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).	Please remove the mandatory country count of 5 or reduce it to 3	Please be guided as per the RFP and its subsequent corrigenda.
68	93	Annexure 16 Pn (3) Technical Functional Specification Compliance for Incident Response Retainer (IRR) Services.	Service provider must release at least 5 reports, media articles, whitepapers on topics related cyber security, information security, attack vectors etc.	Request to remove this clause or reduce the no. of reports to 3.	Please be guided as per the RFP and its subsequent corrigenda.

69	94	Annexure 16 Pn (11) Technical Functional Specification Compliance for Incident Response Retainer (IRR) Services.	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.	Request to remove this clause, as the client's name for DFIR services is not disclosed publicly. Can we provide a declaration as supporting evidence?	Marked details will sufficient
70	94	Annexure 16 Pn (12) Technical Functional Specification Compliance for Incident Response Retainer (IRR) Services.	The Service provider must be recognized by the industry experts and listed minimum once in last three year, in external market research reports published for cyber security incident response by Forrester Wave, Gartner's Magic Quadrant, or International Data Corporation (IDC), Aite-Novarica, IT Central Station etc. for their Digital Forensics and Incident Response (DFIR) services.	Please accept our declaration as supporting for this.	**Clause removed please refer corrigendum.**
71	95	Annexure 16 Pn (15) Technical Functional Specification Compliance for Incident Response Retainer (IRR) Services.	The Service provider must have more than 25 MITRE Attack references.	Request to remove this clause or make is desirable	Desirable instead of mandatory. Please refer corrigendum.
72	95	Annexure 16 Pn (16) Technical Functional Specification Compliance for Incident Response Retainer (IRR) Services.	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.	Request you to remove this clause or reduce the profile count to 5.	Please be guided as per the RFP and its subsequent corrigenda.
73	96	Annexure 16 Pn (20) Technical Functional Specification Compliance for Incident Response Retainer (IRR) Services.	Provide incident response 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.	Please remove this clause or accept the declaration as supporting for this.	Self-declaration may be accepted.

74	95	Annexure 16 (Pn 17) Technical Functional Specification Compliance for Incident Response Retainer (IRR) Services.	The endpoint agent/EDR/solution which bidder is using during assessment/incident response, must be installed and monitored in at least One Lakh Endpoints / Honeypots / Sensors globally	It is requested to clarify if the bidder need to deploy new EDR solution on one lakh endpoints for incident response, in case the Bank already has a EDR solution deployed in the environment?	The bidder does not need to deploy new EDR solution. The agent or solution proposed for the forensics activity need to satisfy the RFP requirements.
75	101	Annexure 17 (in Note Pn 5) Technical Scoring Parameters	Purchase orders should be duly supported by proof of successful execution. Only purchase order will not be considered for scoring	Please clarify what specific documents or evidence are considered acceptable as proof of successful execution in addition to the purchase order (e.g. client confirmation emails, invoices etc	Please be guided as per the RFP and its subsequent corrigendum.
76	105	Annexure 20 Undertaking/Declaration for Support Centre	Undertaking/Declaration for Support Centre	Requesting to include the word "office" also in this clause	Please be guided as per the RFP and its subsequent corrigendum.
77	General Query	General Query	General Query	Is the bidder allowed to transfer the evidence collected from the bank to bidder's forensic lab for further processing and analysis?	Evidence needs to be stored on dedicated forensic workstation/ dedicated IRT infrastructure within India. The system for the evidence needs to be mandatorily encrypted with keys provided to the Bank and necessary Chain-of-custody needs to be preserved during the entire incident lifecycle and beyond.

Punjab National Bank

CENTRALISED PROCUREMENT & PARTNERSHIP DIVISION HO, 5, Sansad Marg, New Delhi – 110 001

Corrigendum -1

RFP for Engaging Services of Incident Response Retainer (IRR).

E-Mail : cppd.processing@pnb.co.in

Web site: www.pnbindia.in

CENTRALISED PROCUREMENT & PARTNERSHIP DIVISION HO, 5, Sansad Marg, New Delhi – 110 001

Corrigendum-1 RFP for Engaging Services of Incident Response Retainer (IRR)

Sr. No.	RFP Page No.	RFP Clause Name & No.	RFP Clause	Amended clause in Corrigendum	Justification
1	94	Annexure 16 Pn (12) Technical Functional Specification Compliance for Incident Response Retainer (IRR) Services.	The Service provider must be recognized by the industry experts and listed minimum once in last three year, in external market research reports published for cyber security incident response by Forrester Wave, Gartner's Magic Quadrant, or International Data Corporation (IDC), Aite-Novarica, IT Central Station etc. for their Digital Forensics and Incident Response (DFIR) services.	Clause removed	For wider participation.
2	95	Annexure 16 Pn (15) Technical Functional Specification Compliance for Incident Response Retainer (IRR) Services.	The Service provider must have more than 25 MITRE Attack references.	Desirable instead of mandatory.	For wider participation.