बैंक ऑफ़ बड़ौदा Bank of Baroda

Pre bid replies – RFP (Request for proposal) for engagement of information Security Consultant: Bid No – GEM/2025/B/5843425 Dated 22nd Jan 2025

Sr. No.	RFP Page No.	Point / Section	Clarification point as stated in the tender document	Comment /Suggestion	Bank's Reply
1	11	Key Domain review & Gap analysis	Bidder shall review and analyse process and operations of bank's Information security department sub-verticals.	Kindly confirm the sub-verticals of the Bank's department the gap assessment needs to be performed for.	Please refer section 2 (Project Overview)
2	11	Key Domain review & Gap analysis	Bidder shall review and analyse process and operations of bank's Information security department sub-verticals.	Kindly confirm which application of the Bank the policy and framework needs to be prepared for.	Please refer RFP
3	11	Key Domain review & Gap analysis	Bidder shall review and analyse risk assessment method, template, and process. Post analysis, bidder shall suggest improvement, new template or process, if required, to put bank's risk assessment process at par with Industry standards.	Kindly confirm whether actual risk assessment of applications needs to be performed.	No need to perform actual risk assessment of applications
4	11	Key Domain review & Gap analysis	Scope includes recommendation regarding requirement of new security solution to further enhance security posture of organization by reducing threat landscape	Kindly confirm whether assistance in implementation of security solution is required	No assistance required regarding implementation of security solutions
5	11	Key Domain review & Gap analysis	Bidder will create cyber incident scenarios, recommendation and recovery procedure for various cyber threats applicable to banking industry (Ransomware, data exfiltration etc.)	Kindly confirm whether Bank already has test cases and documentation around test scenarios or whether bidder needs to create these from scratch.	Bidder need to prepare various cyber incident scenarios

6	12	Key Domain review & Gap analysis	Bidder should review all policies, standard and guideline documents concerning to Information security and perform a comprehensive design-level gap assessment of its Information & Cyber Security Policies and Procedures against the regulatory requirements i.e. guidelines and mandates of RBI, SEBI, NCIIPC, Cert-In & other regulators/government,	Kindly confirm the additional policies and guidelines that are under the scope of this engagement.	Please refer RFP
7	12	Key Domain review & Gap analysis	Scope will also include review and gap assessment of compliance status of Bank's overseas territories and subsidiaries with applicable respective International regulators and their industry-leading standards.	Kindly confirm how many territories are under the scope of the engagement and their names.	Refer section introduction
8	12	Key Domain review & Gap analysis	The scope shall also include creation of new and / or improvement, revision in the existing documents / guidelines / checklists / control list/ dashboard as per compliance with regulators / Government of India.	Kindly confirm whether Bank already has policies in place.	Please refer RFP
9	12	Key Domain review & Gap analysis	The scope shall also include creation of new and / or improvement, revision in the existing documents / guidelines / checklists / control list/ dashboard as per compliance with regulators / Government of India.	Kindly confirm whether it is expected to only recommend / suggest imporvements to the processes / policy documents of the Bank, or whether creation of new policy / processes is also expected.	Please refer relevant RFP section
10	12	Key Domain review & Gap analysis	Scope will also include review and gap assessment of compliance status of Bank's overseas territories and subsidiaries with applicable respective International regulators and their industry-leading standards.	Kindly confirm the international regulatory guidelines under scope of this engagement.	will be provided to L1 bidder.

11	12	Key Domain review & Gap analysis	The scope shall also include creation of new and / or improvement, revision in the existing documents / guidelines / checklists / control list/ dashboard as per compliance with regulators / Government of India.	Kindly confirm which 'dashboard' is referred here.	Please refer RFP
12	13	Gap assessment , Recommendation & Reporting	Review of IS governance structure and recommendation for improving efficiency and effectiveness including development of KPIs, KRIs, KCIs etc.	Kindly confirm whether Bank already has KPIs, KRIs and KCIs in place.	Please refer RFP
13	13	Gap assessment , Recommendation & Reporting	Competency mapping of IS dept. bank staff with suitable recommendation to bridge the gap, if any including training, certification, knowledge transfer and staff realignment.	Kindly elaborate on the expectation from the 'competency mapping".	Please refer RFP
14	14	Gap assessment , Recommendation & Reporting	h. Map the observations identified as part of the gap analysis with the planned initiatives of the Bank.	Kindly elaborate the expectation from this scope item.	Please refer RFP
15	14	3.2 Incident Response Retainer services:	NA	Kindly confirm is this is a loan staffing / secondment form of requirement.	Please refer RFP
16	14	3.2 Incident Response Retainer services:	NA	Kindly confirm the number of resources required for this activity. Elaborate on both online and offline resource requirements.	Bidder to ensure that enough man power and resources are deployed to ensure that incident response services are provided to bank in timely and effective manner. Please refer RFP for details.
17	14	3.2 Incident Response Retainer services:	NA	Kindly confirm whether Bank has required tools to conduct this engagement, or whether bidder is expected to purchase tools.	Bidder is supposed to bring necessary tools to execute the assignment.

18	14	3.2 Incident Response Retainer services:	The IR analyst should be at onsite location of breach, if required, as per following timelines Within India-Tier1 Cities, metropolitan city, State capitals – within 12 hrs Within India- Location other than as mentioned above – within 24 hrs	Kindly confirm whether travel expenses will be covered by the Bank.	Travel expenses, if any should be part of IRR man hour cost.
19	16	3.3 Table top exercise:	3.3.1 Purpose of table top exercises is to understand the roles and responsibilities of the support team, response priorities, and order of events, roles of the various plans, communication requirements, and the role and use of the tools at the team's disposal. Participants also learn how to react to various scenarios, verify procedures and determine what is missing from plans.	Kindly confirm the team for which table top exercise must be conducted.	Bank support team which includes Information secuirty team, IT Team etc.
20	16	3.3 Table top exercise:	Service provider will also conduct table top exercises and attack simulations that involves testing the process outlined in cyber crisis management plan and to ensure that team members know their roles and responsibilities. This activity will be conducted by service provider once in a quarter or as per requirement from Bank.	Kindly confirm applications under the scope of this service.	Please refer RFP

21	16	3.3 Table top exercise:	3.3.2 In addition to this, service provider will also provide table top exercise/simulation exercise to Bank's Top management/ Board members etc. upon the request from the bank. Bidder will create detailed plan that includes the realistic scenario, objectives, roles and responsibilities as part of cyber crisis management.	Kindly confirm number of iterations of training to be provided.	Please refer commercial section (Annexure-11)
22	17	NA	Failure to fulfil agreed-upon timelines/service levels will result in penalties @ one man hour cost for each hour delay in providing IRR services. Failure to provide table top exercise in stipulated time will result in penalty @ 5 percent of table top exercise cost per day.	Kindly confirm whether there is any cap on liability under this statement.	Please refer RFP
23	NA	NA	NA	Kindly confirm the steps to submit the EMD, for both cases: 1. NEFT What date must the transaction be made. What must be attached in the proposal as proof of submission. 2. BG How will BG be submitted in the case on onlin bid submission.	Refer annexure 4 of RFP
24	NA	NA	NA	Which countries are required to be covered for forensic analysis	Domestic Country

25	NA	15	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.	Is the vendor expected to support bank with recommendations for restoring the systems to normal state and remediating the vulnerabilities or they are expected to restore the systems (servers/applications/devices) and remediate vulnerabilities themselves?	Bidder would provide support bank in restoration of bank's servers/infra
26	NA	15	Eradication: This phase involves removing the threat and restoring affected systems to their original state. For example, this may involve deleting malware, applying software patches, recommendation of closing vulnerability, exploit used by the threat actor to gain access to the network or restoring from backups. It should be made sure that eradication of threat is to be carried out without disruption to the business.	Is the vendor expected to support bank with recommendations for eradication or they are expected to eradicate the threats from systems (servers/applications/devices) themselves?	Bidder would provide support in eradication of threats present in bank's servers/infra
27	NA	15	Recovery /monitoring: In this phase, the incident response team will work to restore normal business operations and ensure that all systems are functioning properly.	Would the OPEs (cost of HDDs used for imaging, travel cost, accommodation, etc.) for conducting Forensics be billable separately on actuals?	HDD, Travel cost, accommodation , if any should be made part of Man hour cost
28	NA	NA	NA	What is the cap on number of hours to be proposed for doing Incident response & forensics? How would additional hours consumed on the actual incidents be billed?	Please refer commercial section (Annexure-11)
29	11	3.1	Bidder shall review and analyse process and operations of bank’s Information security department sub-verticals.	What specific sub-verticals within the Information Security Department are to be reviewed and analysed? Can you provide a brief description of each?	Please refer section 2 (Project Overview)
				What are the primary objectives and expected outcomes of this review and analysis?	Please refer RFP

				Is there existing documentation on the processes and operations of the sub-verticals, such as policies, procedures, and process maps?	Yes
				What regulatory compliance standards is the bank subject to, and how do they impact the Information Security Department's operations?	Please refer RFP
				Have there been any previous reviews or audits of the Information Security Department? If so, can the findings or reports be shared?	Not applicable
30	11	3.1	Bidder shall review and analyse risk assessment method, template, and process. Post analysis, bidder shall suggest improvement, new template or process, if required, to put bank's risk assessment process at par with Industry standards.	We understand that review of the Risk Assessment Policy/Procedures needs to be conducted. Conducting Risk Assessment across the Bank is out-of-scope.	Risk assessment need not to be conducted.
31	11	3.1	Bidder will also suggest improvement w.r.t third party vendor risk assessment process and review of existing vendor risk assessment format/template/Contracts/ SLAs etc.	We understand that the review of the Vendor Risk Assessment process needs to be conducted, and conducting Vendor Risk Assessment is out-of-scope. Kindly let us know the counts of Contracts & SLAs are to be reviewed.	Vendor Risk assessment need not to be conducted.
32	11	3.1	Additionally, Risk assessment methodology, process should also be defined for new emerging technology including but not limited to block chain, Generative AI, Machine Learning, Metaverse, Quantum Computing etc.	Can you please share a complete list of Technologies/Aspects for which the Risk Assessment methodology is to be defined.	Please refer RFP

33	11	3.2	Bidder shall review role and functionality of G-SOC tools and evaluate efficiency and efficacy of these security solution in detecting, analysing and mitigation of cyber-threats along with review of current security solution deployment /coverage (with regards to domain coverage ex: network, Endpoints, servers, mail and Cloud) and highlight gaps, if any in current security posture.	Kindly confirm which all G-SOC Tools are implemented and that need to be evaluated for efficiency & efficacy? 1. Security Incidents & Events Management (SIEM) 2. Intrusion Prevention/Detection Systems (IDS/IPS) 3. Firewalls 4. Endpoints Detection & Response (EDR) 5. Vulnerability Management Tools 6. Incident Response Platforms 7. Threat Intelligence Platforms 8. Network Traffic Analysis 9. Forensic Tools 10. Compliance Management	Details will be provided to L1 bidder. (Approx. 20 security solutions are deployed in SOC)
34	12	3.2	Bidder should review all policies, standard and guideline documents concerning to Information security and perform a comprehensive design-level gap assessment of its Information & Cyber Security Policies and Procedures against the regulatory requirements i.e. guidelines and mandates of RBI, SEBI, NCIIPC, Cert-In & other regulators/government,	Can you please provide further details with regards to guidelines & mandates RBI, SEBI, NCIIPC, Cert-In & other regulators/government that needs to be considered?	Please refer RFP
35	12	3.2	Scope will also include review and gap assessment of compliance status of Bank's overseas territories and subsidiaries with applicable respective International regulators and their industry-leading standards.	Can you please share details which all overseas territories and subsidiaries with applicable respective International regulators and their industry-leading standards are to be considered as part of the scope?	Details will be provided to L1 bidder (refer section 1 introduction)

36	11	3.1	Bidder will create cyber incident scenarios, recommendation and recovery procedure for various cyber threats applicable to banking industry (Ransomware, data exfiltration etc.)	Can you please provide an estimate of Cyber Incident scenarios & recovery procedures which would need to be created?	Approx. 20- 25, However exact number to reflect at the time of project execution.
37	14	3.2	Bank is keen to engage with an experienced Vendor to provide Incident Response Retainer Services to the Bank.	Is digital forensics to be performed as part of Incident Response services	Yes. As per scope mentioned in RFP
				Whether Bank will provide the Tools for performing the analysis or the Vendor has to carry the tools	Bidder to arrange from their end
				Whether Bank will provide the Hard Disk space for data collection and storage, if vendor has to carry how long the data should be preserved/retained	Bidder to arrange from their end and should be kept in bank's custody.
				Whether Bank will provide the computer systems for analysis or vendor should use their computer systems	Yes, Bank will provide
				Can vendor carry the collected data to forensic labs to perform the analysis	As per Bank's discretion
38	16	3.3	Purpose of table top exercises is to understand the roles and responsibilities of the support team, response priorities, and order of events, roles of the various plans, communication requirements, and the role and use of the tools at the team's disposal. Participants also learn how to react to various scenarios, verify procedures and determine what is missing from plans.	What should be the duration of each Table top Exercise	The duration of a table top exercise can vary depending on the incident scenario, objectives, complexity, and goals of the exercise. Hence bidder should decide the duration as per Industry best practices.
				Who will provide the Scenarios for Table top Exercise i.e. Bank or the Supplier	End to end Table top exercise should be done by the bidder which includes Scenarios as per Industry best practices and same can be reviewed by the bank.

				Whether the Exercise will be Physical or Virtual	Physical (either at DC - Mumbai, DR-Hyderabad). However bank can decide to go for virtual if such need arises.
				Number of participants for each Tabletop exercise	Approx. 30-40, However Bank has not put any cap on number of participants in RFP.
39	11	3. Scope of work: 3.1 Key Domain review & Gap analysis:	Bidder shall review and analyse process and operations of bank's Information security department sub-verticals.	Are there additional Information security verticals apart from the details highlighted in section: 2. Project Overview of the tender?	All major verticals are illustrated in project overview section.
40	11	3. Scope of work: 3.1 Key Domain review & Gap analysis:	Bidder should also align risk assessment process with specific risk assessment framework i.e ISO 27005, 31000 etc.	Are there any additional regulatory or compliance frameworks the bank requires adherence to?	The point is self-explanatory
41	11	3. Scope of work: 3.1 Key Domain review & Gap analysis:	Bidder will also suggest improvement w.r.t third party vendor risk assessment process and review of existing vendor risk assessment format/template/Contracts/ SLAs etc.	Request the Bank to provide the number of vendors/SLAs that needs to be reviewed.	The point is self-explanatory
42	11	3. Scope of work: 3.1 Key Domain review & Gap analysis:	Bidder will also suggest improvement w.r.t third party vendor risk assessment process and review of existing vendor risk assessment format/template/Contracts/ SLAs etc.	Does the bank have preferred methods/tools for assessing third-party vendor risks?	Bank has set process/templates to assess Vendor risk assessment.

43	11	3. Scope of work: 3.1 Key Domain review & Gap analysis:	Additionally, Risk assessment methodology, process should also be defined for new emerging technology including but not limited to block chain, Generative AI, Machine Learning, Metaverse, Quantum Computing etc.	Request the Bank to elaborate the requirement here. Additionally, what new emerging technologies Bank is using?	Please refer RFP
44	11	3. Scope of work: 3.1 Key Domain review & Gap analysis:	Bidder shall review role and functionality of G-SOC tools and evaluate efficiency and efficacy of these security solution in detecting, analysing and mitigation of cyber-threats along with review of current security solution deployment /coverage (with regards to domain coverage ex: network, Endpoints, servers, mail and Cloud) and highlight gaps, if any in current security posture.	Request the Bank to provide a list of existing G-SOC tools to be reviewed?	We will be provided to L1 bidder. (Approx. 20 tools are deployed in SOC)
45	11	3. Scope of work: 3.1 Key Domain review & Gap analysis:	Bidder will create cyber incident scenarios, recommendation and recovery procedure for various cyber threats applicable to banking industry (Ransomware, data exfiltration etc.)	Any specific types of cyber incidents the bank has faced in the past for contextual reference?	The point is self-explanatory
46	11	3. Scope of work: 3.1 Key Domain review & Gap analysis:	Bidder will create cyber incident scenarios, recommendation and recovery procedure for various cyber threats applicable to banking industry (Ransomware, data exfiltration etc.)	Is the bidder expected to recommend or simulate specific scenarios?	Please refer RFP

47	12	3. Scope of work: 3.1 Key Domain review & Gap analysis:	Bank has Information Security Policy, Cyber Security Policy, CCMP (Cyber Crisis Management Plan) and other 23 Standard and Guideline documents, covering various aspects of Information Security.	Apart from these 26 documents, any additional documents to be added?	Please refer RFP
48	12	3. Scope of work: 3.1 Key Domain review & Gap analysis:	Bank has Information Security Policy, Cyber Security Policy, CCMP (Cyber Crisis Management Plan) and other 23 Standard and Guideline documents, covering various aspects of Information Security.	Are there any particular policies or procedures that have been flagged for immediate improvement or review?	Please refer RFP
49	12	3. Scope of work: 3.1 Key Domain review & Gap analysis:	1. Bidder should review all policies, standard and guideline documents concerning to Information security and perform a comprehensive design-level gap assessment of its Information & Cyber Security Policies and Procedures against the regulatory requirements i.e. guidelines and mandates of RBI, SEBI, NCIIPC, Cert-In & other regulators/government,	Will the bank provide access to prior compliance audit reports or assessments for reference?	Bank to decide at the time of project initiation & execution
50	12	3. Scope of work: 3.1 Key Domain review & Gap analysis:	Scope will also include review and gap assessment of compliance status of Bank's overseas territories and subsidiaries with applicable respective International regulators and their industry-leading standards.	Could you provide details on the overseas territories and subsidiaries in scope, including the number of entities and their regulatory environments?	More Details will be provided to L1 bidder (refer section 1 introduction)

51	12	3. Scope of work: 3.1 Key Domain review & Gap analysis:	Scope will also include review and gap assessment of compliance status of Bank's overseas territories and subsidiaries with applicable respective International regulators and their industry-leading standards.	Are there specific international standards or country-specific regulations that the bidder should prioritize during the gap assessment?	Details will be provided to L1 bidder (refer section 1 introduction)
52	11	3. Scope of work: 3.1 Key Domain review & Gap analysis:	General	Is vulnerability assessment and penetration testing (VAPT) to be conducted for the engagement? If so, will it be internal, external or both? Please do mention the count of the IPs for both internal and external.	Not required
53	11	3. Scope of work: 3.1 Key Domain review & Gap analysis:	General	Is web application testing to be conducted for the engagement? If so, then please mention the count of applications, number of pages in each application.	Not required
54	11	3. Scope of work: 3.1 Key Domain review & Gap analysis:	General	Is mobile application testing to be conducted for the engagement? If so, then please mention the target OS of the application (IOS/android), count of the applications and number of pages in each application.	Not required
55	11	3. Scope of work: 3.1 Key Domain review & Gap analysis:	General	Is secure code review to be conducted for the engagement? If so, then please mention the count of the applications, count of lines of code in each application.	Not required
56	11	3. Scope of work: 3.1 Key Domain review & Gap analysis:	General	Is network architecture review to be conducted for the engagement? If so, whether the branches are to be considered along with HO and then their count as well.	Not required

57	11	3. Scope of work: 3.1 Key Domain review & Gap analysis:	General	Is configuration review to be conducted for the engagement? If so, please specify the count of the unique hosts (OS, DB, network devices, etc.) that are to be reviewed.	Not required
58	11	3. Scope of work: 3.1 Key Domain review & Gap analysis:	General	Is SCD (Secure configuration document) creation to be conducted for the engagement? If so, please specify the count of the unique hosts (OS, DB, network devices, etc.) for which SCDs are to be created.	SCD creation not required. However Bidder can highlight absence of any specific SCD in Bank's environment.
59	11	3. Scope of work: 3.1 Key Domain review & Gap analysis:	General	Will BOB provide the tools for conducting application security (Web/mobile), code review and VAPT or is the partner supposed to get their own tools.	The point is self-explanatory
60	34	1.4 Do's and Don'ts for Bidder	Covering letter certifying compliance of Eligibility criteria and Scope of Work.	Could you let us know what exact document is needed for this point?	Please refer RFP

61	82	27. LIMITATION OF LIABILITY	Except the grounds mentioned under the para two of this clause, Service Provider's aggregate liability in connection with obligations undertaken as a part of the Agreement regardless of the form or nature of the action giving rise to such liability (whether in contract, tort or otherwise), shall be at actual and limited to the Total Contract Value. However, Service Provider's liability in case of claims against the Bank resulting from Willful Misconduct or Gross Negligence of Service Provider, its employees and Subcontractors or from infringement of patents, trademarks, copyrights or such other Intellectual Property Rights or breach of confidentiality obligations shall be unlimited. Bank shall not be held liable for and is absolved of any responsibility or claim / litigation arising out of the use of any third-party software or modules supplied by Service Provider as part of procurement under the Agreement. Under no circumstances BOB shall be liable to the Service Provider for direct, indirect, incidental, consequential, special or exemplary damages arising from termination of this Agreement, even if BOB has been advised of the possibility of such damages, such as, but not limited to, loss of revenue or anticipated profits or lost business. Subject to any law to the contrary, and to the maximum extent permitted by law neither parties shall be liable to other for any consequential/ incidental, or indirect damages arising out of this agreement.	1. Please suggest the following modification to Clause 27 ('Limitation of Liability'), provided on Page 82 of the RFP: Except the grounds mentioned under the para two of this clause, Service Provider's aggregate liability in connection with obligations undertaken as a part of the Agreement regardless of the form or nature of the action giving rise to such liability (whether in contract, tort or otherwise), shall be at actual and limited to the Total Contract Value. Bank shall not be held liable for and is absolved of any responsibility or claim / litigation arising out of the use of any third-party software or modules supplied by Service Provider as part of procurement under the Agreement. Under no circumstances BOB shall be liable to the Service Provider for direct, indirect, incidental, consequential, special or exemplary damages arising from termination of this Agreement, even if BOB has been advised of the possibility of such damages, such as, but not limited to, loss of revenue or anticipated profits or lost business. Subject to any law to the contrary, and to the maximum extent permitted by law neither parties shall be liable to other for any consequential/ incidental, or indirect damages arising out of this agreement. All employees engaged by the party shall be in sole employment of the party and the respective parties shall be solely responsible	No change

			All employees engaged by the party shall be in sole employment of the party and the respective parties shall be solely responsible for their salaries, wages, statutory payments etc. That under no circumstances shall other party be liable for any payment or claim or compensation (including but not limited to compensation on account of injury/death/termination) of any nature to the employees and personnel of the other party.	for their salaries, wages, statutory payments etc. That under no circumstances shall other party be liable for any payment or claim or compensation (including but not limited to compensation on account of injury/death/termination) of any nature to the employees and personnel of the other party.”	
62	75	17. CONFIDENTIALITY	b) Service Provider shall not make or retain any copies or record of any Confidential Information submitted by BOB other than as may be required for the performance of Service Provider.	Please acknowledge : Notwithstanding anything to the contrary, Service Provider shall be allowed to retain sufficient documentation as part of its professional records to support and evidence the work performed by the Service Provider. Such retention shall be subject to obligations of confidentiality mentioned herein.	No change

63		26. AUDIT	All Service Provider records with respect to any matters covered by this Agreement shall be made available to auditors and or inspecting officials of the Bank and/or Reserve Bank of India and/or any regulatory 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. Said records are subject to examination. Bank's auditors would execute confidentiality agreement with the Service Provider provided that the auditors would be permitted to submit their findings to the Bank, which would be used by the Bank. The cost of the audit will be borne by the Bank. The scope of such audit would be limited to Service Levels being covered under the contract, and financial information would be excluded from such inspection, which will be subject to the requirements of statutory and regulatory authorities. The Bank and its authorized representatives, including Reserve Bank of India (RBI) or any other regulator shall have the right to visit any of the Service Provider's premises without prior notice to ensure that data provided by the Bank is not misused. The Service Provider shall cooperate with the authorized representative/s of the Bank and shall provide all information/ documents required by the Bank.	Request the team for inclusion of the below details : "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 Service Provider'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 Bank and be discussed and agreed mutually between the Bank and the Service Provider for its closure."	No change
64	14	3.2 Incident Response Retainer services:	3.2 Incident Response Retainer services:	Could you explain the schedule of this service? Is it after the gap assessment service for next 2 years?	Please refer RFP

65		NA	General	Please confirm, we need to conduct the gap assessment from Bank's office or can it be performed remotely?	Bank's Office premise
66		NA	General	Please provide count of servers, network devices, policies , procedures, etc.	Please refer RFP
67		NA	General	Please confirm, for gap assessment, is the bidder allowed to do hybrid work post conducting assessment for report/document submission.	Bank's Office premise
68	39	Annexure 02 - Evaluation Terms Technical, Experience and Support	Supporting Documents Required: Letter of confirmation from the bidder (as per format provided in the RFP) duly signed by authorized official of the bidder, along with copy of engagement letter/work order/letter of award for each assignment.	Please confirm whether only purchase order will suffice the criteria.	Letter of confirmation from the bidder (as per format provided in the RFP) duly signed by authorized official of the bidder, along with copy of engagement letter/work order/letter of award for each assignment.
69	41	B. Technical Bid Evaluation	Essential Resources and Expertise Needed: Qualified professionals holding CISA/CISM/CISSP / CRISC / ISO 27001 Certification, expertise in Gap Analysis, Risk Assessment, and IT Outsourcing domains, or equivalent certified personnel, must be employed full-time by the Bidder < 50 Employees – No marks 50 – 100 Employees – 5 marks >100 Employees – 10 marks	Request you to reduce the number of resources as sharing all certificates would not be feasible	Qualified professionals holding either CISA/CISM/CISSP / CRISC / ISO 27001 Certification

70	11	3.1 Key Domain review & Gap analysis: 1. Bidder shall review and analyse risk assessment method, template, and process. 2,Bidder will also suggest improvement w.r.t third party vendor risk assessment process and review of existing vendor risk assessment format/template/Contracts/SLAs etc.		1. Bidder is expected to review OR creation of the new RA methodology and templates. Please clarify. 2. Bidder is expected to review the existing templates and process and will make suggestion. There will be no formulation of the new documents. Please clarify	Please refer RFP
71	11	3.1 Key Domain review & Gap analysis:	Bidder shall review role and functionality of G-SOC tools	How many SOC tools are available with the Bank, whether the review will be based on the sample SOC tools or the entire list of tools?	20+ SOC tools are available with the Bank. Review should be done for all tools.
72	11	3.1 Key Domain review & Gap analysis:	Bidder will create cyber incident scenarios, recommendation and recovery procedure for various cyber threats applicable to banking industry (Ransomware, data exfiltration etc.)	Pl clarify the expectation. It is part of the BCP/DR…whether this is part of the scope. If yes how many scenarios to be considered (clarify)	Approx. 20- 25 However exact number to reflect at the time of project execution.
73	11	3.1 Key Domain review & Gap analysis:	Bidder should review current training material and programme, periodicity, scope,	Only review will be conducted, creation of training material is not in scope. Please clarify	Yes. Only review will be conducted with recommendations

74	11	Scope will also include review and gap assessment of compliance status of Bank's overseas territories and subsidiaries with applicable respective International regulators and their industry-leading standards.	Scope will also include review and gap assessment of compliance status of Bank's overseas territories and subsidiaries with applicable respective International regulators and their industry-leading standards.	1. Is gap assessment against existing Bank's policies and procedures part of the scope across all international territories? 2. Whether Data will be provided to us for conducting gap assessment for Int. Territories 2. How many Interiorizes are active for BoB? 2. Formulation of the new policies / processes part of the scope?	Please refer RFP
75	11	The scope shall also include creation of new and / or improvement, revision in the existing documents / guidelines / checklists / control list/ dashboard as per compliance with regulators / Government of India.	The scope shall also include creation of new and / or improvement, revision in the existing documents / guidelines / checklists / control list/ dashboard as per compliance with regulators / Government of India.	Dashboard as per compliance with regulators / Government of India….what is the expectation from the bidder?	Please refer RFP

76	11	To understand each domain functions, process. Perform a design-level assessment for each domain determine the current status of the dept. function and process and identify non-conformities and the associated information security risks. This exercise (review of Information security department activities & operations) is one time activity.	To understand each domain functions, process. Perform a design-level assessment for each domain determine the current status of the dept. function and process and identify non-conformities and the associated information security risks. This exercise (review of Information security department activities & operations) is one time activity.	Gap assessment against the existing CISO departments functions…please clarify Is compliance part of the activity	Please refer RFP
77	11	Benchmarking of Bank's Cyber security posture with peers PSB Banks as wells as private sector banks.	Benchmarking of Bank's Cyber security posture with peers PSB Banks as wells as private sector banks.	Cyber Maturity Assessment based on NIST framework is the Ask? Pl clarify	Please refer RFP

78	11	Methods and procedure to calculate bank's cyber risk in monetary terms by using internation al risk quantificati on models (FAIR model etc.)	Methods and procedure to calculate bank's cyber risk in monetary terms by using international risk quantification models (FAIR model etc.)	What's is the expectation? Please clarify	Please refer RFP
79	11	Develop a prioritized implementa tion roadmap with timelines post discussion with the stakeholder s.	Develop a prioritized implementation roadmap with timelines post discussion with the stakeholders.	Implementation roadmap for which of the scope line item? Please elaborate.	Please refer RFP
80	11	Compliance check on actions taken to attend identified gaps & recommend ations and publication of final closure report.	Compliance check on actions taken to attend identified gaps & recommendations and publication of final closure report.	Compliance assessment for which scope line item? One time compliance will be carried out	Please refer RFP

81	11	The IR analyst should be at onsite location of breach, if required, as per following timelines Within India-Tier1 Cities, metropolitan city, State capitals – within 12 hrs Within India- Location other than as mentioned above – within 24 hrs	The IR analyst should be at onsite location of breach, if required, as per following timelines Within India-Tier1 Cities, metropolitan city, State capitals – within 12 hrs Within India- Location other than as mentioned above – within 24 hrs		The point is self-explanatory
82	4	4. Contract period		Entire contract period for 2 years or for IR retainer and Table top will be two years	Entire contract period is for 2 years