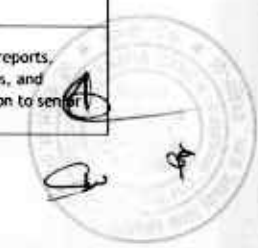


Replies to Prebid queries to GeM bid ref: GEM/2025/B/6840553 dated 30/10/2025 for Selection of Cert-In Empanelled Auditor for Conducting Comprehensive Security Assessment of IT Architecture & IT Infrastructure in Canara Bank

Sl. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1	13	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	1 Project Timelines	1.2 The entire Assessment process has to be completed within 9 months from the date of acceptance of the Purchase Order.	Given our experience working with Canara Bank and given the scope of the RFP, it will not be possible to complete the work in 9 months. Therefore, we request you to put the end date as 15 Months.	Bidder to comply with RFP terms and conditions. The project is structured into 3 phases, however bidders have the option to implement all the phases concurrently.
2	13	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	1 Project Timelines	1.3 The selected bidder to keep the following timelines in regard to the completion of Assessment	Similarly, timelines needs to be stretched to 9, 12 and 15 Months for phase 1, 2 and 3 respectively	Bidder to comply with RFP terms and conditions. The project is structured into 3 phases, however bidders have the option to implement all the phases concurrently.
3	15	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	2. Payment Terms	2.1. The payment schedule will be as under and will release after execution of contract agreement:	Kindly revise the payment milestone as below: Completion of assessment and report submission for respective phase after deducting Liquidated Damages (if any) as per RFP Terms & conditions. - 70% of Invoice Value of respective Phase Re-assessment of all the observations marked as Critical & High and 25% of remaining observations on a random basis for respective Phase after deducting Liquidated Damages (if any) as per RFP Terms & conditions. - 15% of Invoice Value of respective Phase After completion of all phases and acceptance of the same by Bank, deduction towards applicable penalties and Liquidated damages (if any) as per RFP Terms & conditions. - 15% of the Invoice Value of respective Phase Note: Observations for re-assessment needs to be provided within 2 months from the completion of assessment. Otherwise, bidder will mark it as complete and raise the invoice.	Bidder to refer to Corrigendum-1
4	16	3.	3.1 Liquidated Damages for non-delivery of Services:	If the Assessment is not completed within the Phase wise timelines as per clause no.1.3 of section C, Bank will impose penalty @0.50% per week delay and part thereof on the total cost of respective phase. However, the total Penalty/LD to be recovered shall be restricted to 10% of total cost mentioned in Annexure 15(Bill of Material).	Bidder will be sharing the pre-requisites for each domain in phase wise manner. Bidder requires to receive the details within 2 weeks from the date of sharing of the pre-requisites. In case, bidder cannot receive the details, bidder will be marking it as Not Available. Otherwise, bidder should not be held responsible for LD.	Bidder to comply with RFP terms and conditions.
5	56	Annexure-2	6 - The Bidder should have conducted at least 30 out of 40 (Sub-Domains to be considered) Assessments mentioned under the scope of work in Annexure 8, during the last three years as on the submission of Bid in BFSI sector organization/ Scheduled Commercial Banks/ Government Departments/ PSU organization in India.	The Bidder has to provide purchase order copy / reference Letter in their name from BFSI sector organization / Scheduled Commercial Banks / Government Departments / PSU organization in India duly mentioning the assessment carried out along with invoice.	Please allow bidder to provide Engagement Contract Letter on bidder letter head to show compliance to domains. We understand only PO/ Engagement Contract/ Reference Letter should suffix the requirement.	Bidder to refer Corrigendum-1 and comply with RFP terms and conditions.



6	70	Annexure-8 Scope of Work	Assess mobile app security against OWASP Mobile- Top 10	5.1 Application, Web, Mobile & API Security	We understand bidder is not required to perform any VAPT activities be it Web, Mobile, Infrastructure, API or Cloud Review as part of this RFP. Bidder will be looking at the process to understand if existing VAPT is following OWASP standard.	As part of the Comprehensive Security Assessment of all IT assets, the bidder is required to evaluate the existing VAPT process for the mobile application to ensure that it aligns with OWASP Mobile Top 10 standards and best practices.
7	71	Annexure-8 Scope of Work	Review on threat modelling practices in alignment with the threat modelling framework (STRIDE, OWASP, etc.)	5.5. Threat Modelling and threat hunting Point : a	We understand bidder is not required to perform any Threat Modeling activities as part of this RFP. Bidder will be looking at the process to understand if existing process and identify gap in the process.	The bidder is expected to review the existing threat modelling practices to assess alignment with recognized frameworks such as STRIDE and OWASP, and identify any gaps or areas for improvement in the current process.
8	77	Annexure-8 Scope of Work	Identify bank cloud assets (IaaS, PaaS, SaaS), review secure configuration and posture using frameworks (CIS, OWASP).	14.2 Cloud Security Assessment Point : a	Is the expectation from bidder to perform configuration review of cloud assets. If yes, will bank be providing Tenable license to bidder to perform the review. Additionally, bidder is required to understand the asset count for the review.	The bidder is expected to review the existing secure configuration of identified cloud assets (IaaS, PaaS, SaaS) against relevant frameworks such as CIS and OWASP. The asset count and related details will be shared by the Bank during the assessment.
9	78	Annexure-8 Scope of Work	Inventory and classification of AI/ML models used across business processes	15.1 AI/ML Security Point : a	Kindly confirm whether the Bank is currently utilizing any AI/ML models developed in-house for training purposes, or if it is leveraging third-party AI models across its business processes	Details will be shared with selected bidder
10	78	Annexure-8 Scope of Work	Assessment of model training data integrity and data poisoning threats	15.1 AI/ML Security Point : b	Kindly confirm whether the Bank is currently utilizing any AI/ML models developed in-house for training purposes, or if it is leveraging third-party AI models across its business processes	Details will be shared with selected bidder
11	78	Annexure-8 Scope of Work	Security reviews of robotic process automation (RPA) and AI/ML toolchains.	15.1 AI/ML Security Point : d	Could you confirm whether the Bank is currently using Robotic Process Automation (RPA) in its operations or is it outsourced?	Details will be shared with selected bidder
12	80	Annexure-8 Scope of Work	Considering the control points in the above-mentioned domains, the assessment has to be conducted for all the applications of the Bank.	Coverage of the Assessment	Considering the control areas mentioned above, please provide a list of all applications that are in scope for the assessment. Also, help us with the number of switches, Servers, APIs for the environment.	Details will be shared with selected bidder
13	84	Annexure-9 Technical Eligibility Criteria	Technical Eligibility Criteria	* The bidder has to provide relevant purchase order / work order / engagement letter along with satisfactory project completion certificate/ Reference letter from the Concerned Organization /Email reference from the client	Please allow bidder to provide Purchase order or Engagement Contract along with Invoice or Completion Certificate or Mail from Client. We will adhere to this point - Kindly note that that Client's Email should be from their official Email IDs only, containing their name, designation & Contact number.	Bidder to refer Corrigendum-1
14	67	Annexure-8 Scope of Work	1.3. Identity & Access Management	Review AD (Active Directory) Structure: =Review the Organization and Structure of AD domains, forests, and OUs =Assess the configuration of domain including the roles and responsibilities	How many GPOs are currently active, and are there any baseline or security-specific GPOs applied universally? Also How many AD domains are there currently in Bank?	Details will be shared with selected bidder
15		Other queries			Bidder will be sharing the pre-requisites for each domain in phase wise manner. Bidder requires to receive the details within 2 weeks from the date of sharing of the pre-requisites. In case, bidder cannot receive the details, bidder will be marking it as Not Available.	Bidder to comply with RFP terms and conditions.
16	14	Section C	Deliverables		Kindly confirm the expected format of deliverables (reports, dashboards, executive summary, risk heatmaps) and whether presentations to senior management / CISO are expected as part of final submission.	Deliverables shall include detailed reports, executive summaries, risk heatmaps, and dashboards, with a final presentation to senior management and the CISO.



17	66	Annexure-8	Scope of Work	General	Kindly confirm the total number of applications, IT infrastructure components, and locations (CX, DRC, NDC, regional offices, branches, ATMs, etc.) to be covered in the assessment for appropriate effort estimation.	Details will be shared with selected bidder
18	66	Annexure-8	Scope of Work	Note	The RFP mentions use of Agentic AI for improving accuracy and real-time insights. Kindly clarify if the Bank expects demonstration of specific AI/automation tools, or if bidders can propose their own approach.	Bidders may propose their own AI or automation-based approach to demonstrate the use of Agentic AI for improving accuracy and real-time insights
19	66	Annexure-8	Additional Scope of Work	Point 1	Kindly specify the minimum number of resources to be deployed and whether remote/hybrid mode delivery is permissible for certain assessment activities.	As it is a time bound activity, adequate no of resources shall be deployed onsite for the assessment.
20	66	Annexure-8	Section 1	1.1 - IT Asset, Inventory & Endpoint Management	Please provide the approximate count of endpoints (servers, desktops, laptops) and asset management tools currently in use for scoping.	Details will be shared with selected bidder
21	66	Annexure-8	Section 1	1.3 - Identity & Access Management	Please confirm the number of Active Directory domains/forests and whether privileged access management solutions are already implemented.	Details will be shared with selected bidder
22	66	Annexure-8	Section 2	2.2 - Infrastructure & Data Centre Assessment	Kindly confirm the number and locations of Data Centres, Near DR, and DR sites to be covered and whether physical visits are mandatory.	Details will be shared with selected bidder
23	66	Annexure-8	Section 3	3.1 - Core Banking System (CBS) Assessment	Please confirm whether CBS and Payment Infrastructure assessments will include third-party vendor systems, and if coordination support will be provided by the Bank.	YES, CBS and Payment Infrastructure assessments will include third-party vendor systems. Bank will provide coordination support.
24	66	Annexure-8	Section 3	3.3 - API & Partner Banking Assessment	Please clarify the number of APIs / partner integrations to be reviewed and whether testing environments and credentials will be shared.	Details will be shared with selected bidder
25	66	Annexure-8	Section 4	BCP & DR Assessment	Please confirm the frequency and scope of DR drills to be reviewed and whether observation during a live drill is expected.	The frequency of DR Drill is on half-yearly basis. Yes, observation during a live drill is expected.
26	66	Annexure-8	Section 5.1 - 5.5	Application Security, Threat Modelling & Red Teaming	Please clarify whether Red Teaming / Breach and Attack Simulations should be conducted as live controlled exercises or documentary/process assessments only.	The bidder has to review existing Red Teaming and Breach & Attack Simulation (BAS) simulation practices; no live or controlled attack exercises are to be performed
27	66	Annexure-8	Section 5.5	Threat Modelling & Threat Hunting	Kindly confirm if the Bank expects a tool based threat modelling exercise (e.g., STRIDE, DTD) or manual framework review.	The bidder is expected to review the existing threat modeling practices to assess alignment with recognized frameworks such as STRIDE and OWASP, and identify any gaps or areas for improvement in the current process.
28	66	Annexure-8	Section 6	Cryptography & Data Classification Assessment	Please indicate the ISM and key management solutions deployed for review and whether quantum-safe readiness is limited to documentation review.	Details will be shared with selected bidder.
29	66	Annexure-8	Section 8	GRC & Regulatory Assessment	Kindly confirm if the assessment is expected to include policy and framework alignment workshops with senior management, or purely document review.	The assessment will primarily involve a comprehensive document review to evaluate policy and framework, to validate understanding and gather additional insights.
30	66	Annexure-8	Section 9	ATM, PUM & Cash Management Security	Please specify the number of ATMs/PUMs/cash recyclers in scope and whether physical assessment or remote validation is required.	Details will be shared with selected bidder.
31	66	Annexure-8	Section 10	Digital Banking Channels 10.1 - 10.5	Please provide details on number of Internet Banking, Mobile Banking (Retail / Corporate), CBDC, and Digital Lending applications in scope, and clarify whether source code / UAT access will be provided.	Details will be shared with selected bidder.



32	67	Annexure-8	Section 12	SOC Maturity & Incident Response Assessment 12.1 - 12.2	Please confirm whether the Bank has already implemented SIEM, SOAR, UEBA, TIP, Anti-Phishing, Brand Abuse, and Dark Web Monitoring tools and expects configuration review or readiness evaluation. Yes	Details will be shared with selected bidder
33	67	Annexure-8	Section 13	Database Security Assessment	Please specify the types and approximate count of databases (Oracle, MSSQL, MySQL, PostgreSQL, etc.) and if testing will be done on production or replica environments.	Details will be provided with selected bidder. Bank will not be sharing any CSPM tool outputs
34	67	Annexure-8	Section 14.2	Cloud Security Assessment	Please confirm the cloud service providers (AWS, Azure, GCP, OCI, etc.), number of accounts/workloads, and whether CSPM tool outputs will be shared.	Details will be shared with selected bidder
35	67	Annexure-8	Section 15	AI / ML & Container Security Assessment 15.1 - 15.2	Please clarify whether AI/ML models and container platforms (Kubernetes, OpenShift, Docker) are live in production, and the extent of source access available for review.	Details will be shared with selected bidder
36	67	Annexure-8	Section 16	Social Media & Corporate Website Assessment	Please share the number of official social media accounts and websites/subdomains in scope for assessment.	Details will be shared with selected bidder
37	67	Annexure-8	Section 17.1	Third-Party & Supply Chain Assessment	Kindly confirm if on-site assessment of critical vendors / MSPs / MSSPs is expected, or only review of documentation and SLAs.	The assessment will include on-site reviews of critical vendors, MSPs, and MSSPs, in addition to the evaluation of documentation, SLAs, and supporting evidence, as defined in the scope of work.
38	67	Annexure-8	Section 17.5	MDM Security & IT Awareness Assessment	Please specify the MDM solution deployed, and whether the social engineering exercise should include phishing, vishing, or physical intrusion testing.	Details will be shared with selected bidder
39	81	Annexure-8	Scope of Work	Considering the control points in the above-mentioned domains, the assessment has to be conducted for all the applications of the Bank.	Kindly clarify if the effectiveness of the subdomains can be assessed using sampling method for evidences	Yes sampling method can be adopted
40	81	Annexure-8	Additional Scope of Work	Point 2	Please clarify if permanent on-site presence at Bengaluru is required throughout the assessment or only during specific phases (kick-off, validation, final presentation). Since the RFP states that 'non-compliance to any scope will automatically disqualify the bidder', please confirm if minor methodology or tool deviations may be accepted with justification during technical evaluation.	The resource has to be present on-site at Bangalore is required during the entire assessment
41	81	Annexure-8	Note			Bidder to comply with RFP terms
42	82	Annexure - 9	Technical Eligibility Criteria	Bidder shall be awarded the following scores depending on the number of references bidder showcases in the past 3 years as on the date of submission of Bid -1 or more reviews - 30 +2 reviews - 25 +1 review - 15	request you to modify the clause across all the domain as Bidder shall be awarded the following scores depending on the number of references bidder showcases in the past 3 years as on the date of submission of Bid -2 or more reviews - 30 +1 reviews - 25"	Bidder to refer Corrigendum-1
43	82	Annexure - 9	Technical Eligibility Criteria	Bidder shall be awarded the following scores depending on the number of references bidder showcases in the past 3 years as on the date of submission of Bid -3 or more reviews - 30 +2 reviews - 25 +1 review - 15	for a references of same client for same scope of work carried out in 3 consecutive years will be considered as 1 reference or 3 reference.	Bidder to refer Corrigendum-1. References from the same client for the same scope of work carried out in three consecutive years may be considered as three separate references, provided that each engagement was executed under a distinct contract or renewal cycle.
44	87	Annexure-10	Technical Evaluation Criteria	The Bidder should be a CERT in empanelled vendor continuously for last 5 years (2020-2025) and as on date of submission of Bid.	Request you to modify the clause as "The Bidder should be a CERT in empanelled vendor continuously for last 3 years (2022-2025) and as on date of submission of Bid."	Bidder to refer Corrigendum-1. Bidder to comply with RFP terms and conditions



45	87	Annexure-10	Technical Evaluation Criteria	The Bidder has to provide purchase order copy / reference letter in their name from BFSI sector organization / Scheduled Commercial Banks / Government Departments / PSU organization in India duly mentioning the assessment carried out along with invoice	request you to modify the clause as "The Bidder has to provide purchase order copy / reference letter in their name from BFSI sector organization / Scheduled Commercial Banks / Government Departments / PSU organization in India duly mentioning the assessment carried out"	Bidder to refer Corrigendum-1. Bidder to comply with RFP terms and conditions.
46	Generic	Generic	Generic	Generic	Request you to kindly consider the following clause during the SLA/agreement stage if security testing is in scope: The provisions of this Section apply to Testing Services. Testing Services include scanning, penetration, intrusion testing or related analysis of the Client's information systems or enterprise whether by using intrusive or passive techniques and software tools. The Client hereby consents to EY performing the Testing Services and shall obtain all necessary consents of third party service providers of the Client to such Testing Services. If the Testing Services will be performed with respect to any information systems, applications or components that are hosted by any third party such as an internet service provider or application service provider then the consent shall be in the form separately provided by EY to the Client at the latter's request. The Client understands that Testing Services may result in disruptions of and/or damage to the Client's or third party's information systems and the information and data contained therein, including but not limited to denial of access to a legitimate system user, automatic shut-down of information systems caused by intrusion detection software or hardware, or failure of the information system. The Client is solely responsible for understanding the testing steps that will be performed as part of the Testing Services and for arranging alternative means of operation should such disruptions, or failures occur and for all damage caused by the Testing Services. Kindly confirm if revalidation/retesting to be conducted. If yes how many rounds are expected	RFP clauses are self explanatory. Bidder to comply with RFP terms and conditions.
47	NA	NA	NA	NA	Kindly confirm if revalidation/retesting to be conducted. If yes how many rounds are expected	RFP clauses are self explanatory. Bidder to comply with RFP terms and conditions.
48	NA	Annexure-8	Scope of Work	Application Security, Configuration B Threat Modelling Assessment	Total Number of web and mobile applications in scope ?	Details will be shared with selected bidder
49	NA	Annexure-8	Scope of Work	Application Security, Configuration B Threat Modelling Assessment	Total Number of API in scope ? (Public and Internal)	Details will be shared with selected bidder
50	NA	Annexure-8	Scope of Work	Red Teaming	Does red teaming include physical red teaming ? If yes please specify number of locations.	No - Red Teaming in this engagement does not include physical (live) red teaming exercises
51	NA	Annexure-8	Scope of Work	Application Security, Configuration B Threat Modelling Assessment	Total number of assets in scope for infrastructure VAPT ?	Details will be shared with selected bidder
52	NA	Annexure-8	Scope of Work	Scope of Work	As security testing requires machines/devices with specific configurations (Rooted / Jailbroken Devices) and operating systems (Kali Linux), kindly confirm which party will be responsible for provisioning the necessary testing infrastructure, including the security testing workstation(s) for onsite activities.	Bidder to comply with RFP terms and conditions.
53	1	Bid Details Table		Bid End Date/Time	Request to extend till 02nd December 2025, in order to assess the potential conflict of interest	Bidder to comply with RFP terms and conditions.
54	4	Bid Details Table		Time allowed for Technical Clarifications	Request for a 2nd round of discussion owing to questions arising out of pre-bid discussion preferably 21st November 2025	Bidder to comply with RFP terms and conditions.



55	12	Section B	Clause 5.1	Requirement Details	Duration for conducting the comprehensive assessment is mentioned as 09 months. The timeline of execution could be subjected to be revised based on the project plan / engagement plan upon selection of the bidder, considering there are further data points to be obtained to arrive at a definitive timeline as per point no 5.3 in the section.	Bidder to comply with RFP terms and conditions. The project is structured into 3 phases, however bidders have the option to implement all the phases concurrently.
56	12	Section B	Clause 5.3	Requirement Details	Detailed implementation plan will be discussed and agreed by the bank. However on the last line it states the selected Bidder has to comply with the timelines mentioned.	Bidder to comply with RFP terms and conditions.
57	13	Section B	Clause B 1.8.2, 8.3 & 8.4	Scope of Work	Upon award of the contract, the selected bidder shall submit a vendor-wise detailed execution plan, which will be finalized through mutual agreement. In the event of any deviation from the agreed plan, or if a vendor is unavailable on the scheduled date, the Bank shall provide the Selected Bidder with a minimum of seven (7) days' prior written notice to facilitate the audit.	
58	14	Section C	Clause 1.1	Acceptance of Purchase order	As mentioned by the bank, the broad scope is mentioned, further details for performing the SOW shall be shared by the bank. This will be required for us to start the engagement at the earliest.	The term "rules and conditions" refers to the Bank's internal policies, procedures, guidelines, and compliance requirements
59	14	Section C	Clause 1.2	Timelines for conduction assessments	8.4.2 - Implementation team should be conversant with all rules and conditions to resolve the issues, if any. (Request the bank to clarify what is meant by rules and conditions)	Bidder to comply with RFP terms and conditions.
60	14	Section C	Clause 1.3	Table containing Phases	Acceptance of purchase order timeline to be revised to "To be accepted within 10 working days from the date of PO" requires deeper understanding on what data is available and where the support is required.	Bidder to comply with RFP terms and conditions.
61	14	Section C	Clause 1.3	Table containing Phases	Phase 1 involves critical items request the extension to 6 months. Considering business critical crown jewels are in place along with capacity management for next 3-5 years. This will involve multiple discussions with different stakeholders internally within the bank and the work alongside the change management schedule. (Subject to timely support from bank and vendor)	Bidder to comply with RFP terms and conditions.
62	14	Section C	Clause 1.3	Table containing Phases	The specifics mentioned for each scoper particular in Scope of Work should that be primarily regarded as the only control to be evaluated?	The bidder is expected to evaluate all relevant controls associated with each scope area to ensure a comprehensive assessment in line with industry best practices and regulatory expectations.
63	14	Section C	Clause 1.3	Table containing Phases	As mentioned in coverage of assessment under SoW in page 70/133. What is the total number of web and mobile applications to be considered to be in scope for the mentioned assessment	Details will be shared with selected bidder
64	14	Section C	Clause 1.3	Table containing Phases	Phase 1 - Clarity on how many APIs are present for Core Banking and Payment Infrastructure. This is owing to the fact that the	Details will be shared with selected bidder
65	14	Section C	Clause 1.3	Table containing Phases	Total number of Applications (Web & Mobile), Total number of APIs to be tested are required to arrive an estimate cost	Details will be shared with selected bidder
					Phase 2, Endpoint, Identity & Email Security Assessment mentions further specificity on 66/133 under 1.1.d to focus on "one data center, one near disaster recovery and one disaster recovery center." - Whats the location to be considered	The location are Bangalore and Mumbai



66	14	Section C	Clause 1.3	Table containing Phases	Phase 2 - point no. 8, Application Security, Configuration and Threat Modelling Assessment, further specified in 5.1.e - has a point which is marked as TBD. Recommendations on usage of Indian proxy IPs to connect to delivery channels from blacklisted countries. TBD	Bidder to refer Corrigendum-1 issued for Scope of Work Annexure-8 table No: 5.1.
67	14	Section C	Clause 1.3	Table containing Phases	Phase 2 - point no. 8, Application Security, Configuration and Threat Modelling Assessment, further specified in 5.2.b - use automation for drift detection. Kindly provide clarity if the bank has any existing automation in place	Details will be shared with selected bidder
68	14	Section C	Clause 1.3	Table containing Phases	Phase 2 - point no. 9, ATM, PUM & Cash Management Security Assessment. Sample based assessment to be conducted? If yes, how many ATM machines to be considered & similarly for others. (In line with SOW mentioned in page 73/133)	Sample based assessment to be conducted, the count of the ATM machines would be provided to the selected bidder
69	14	Section C	Clause 1.3	Table containing Phases	Phase 2 - point no. 10, How many different type of DBs does the bank have and instance count per application are available in PROD. (In line with SOW mentioned in page 75&76/133)	Details will be shared with selected bidder
70	14	Section C	Clause 1.3	Table containing Phases	Phase 2 timelines requested to be moved to 09 months from the date of acceptance of purchase order. (Subject to timely support from bank and vendor)	Bidder to comply with RFP terms and conditions. The project is structured into 3 phases, however bidders have the option to implement all the phases concurrently.
71	14	Section C	Clause 1.3	Table containing Phases	Phase 1 timelines requested to be moved to 12 months from the date of acceptance of purchase order. (Subject to timely support from bank and vendor). As this has interdependencies across earlier phases with regards to SOC / Website and vendor assessments, (as mentioned in SOW 79/133 & 80/133)	Bidder to comply with RFP terms and conditions. The project is structured into 3 phases, however bidders have the option to implement all the phases concurrently.
72	14	Section C	Clause 1.4	Assessment to be done on-premise	On-premise refers to Canara Bank HQ premises? Kindly confirm	Yes at Bangalore.
73	14	Section C	Clause 1.8	Timeframe of RFP	Request to revise the timeframe of assessment owing to dependency with the bank and vendors. Also interdependencies within the assessment. Proposed Payment Terms - 70% upon submitting the initial draft report for respective phase - 20 % upon re-assessment of respective phase - 10% upon submission of final report	Bidder to comply with RFP terms and conditions.
74	15	Section C	Clause 2	Payment terms		Bidder to refer to Corrigendum-1
75	16 & 17	Section C	Clause 3.1 & Clause 3.5	Penalties / Liquidated Damages	(Considering the total number of vendors and dependency on both the vendor's point of contact and information from relevant canara bank department, Request to consider lowering the penalties / LD to 0.5% of the per unit vendor pricing and limiting to maximum 7.5% increase the issue is solely on the bidder. If incase the delay is due to obtaining the relevant information from vendor / bank (including staff) the same is not applicable.	Bidder to comply with RFP terms and conditions.





76	17	Section C	Clause 3.4	Cancel the order in the event of delay and invoke performance security	<p>We would request the bank to add below at the end of the clause:</p> <p>In the event that a delay is not attributable to the Auditor and the project requires an extension with additional man-days to complete the audit, the Bank shall compensate the Auditor for the additional man-days based on the mutually agreed fee structure. In case the applicable fees cannot be mutually concluded, the Bidder shall reserve the right to cancel the Order.</p>	Bidder to comply with RFP terms and conditions.
77	17	Section C	Clause 3.1	Penalties / Liquidated Damages	<p>We would request the Bank to add below at the end of the clause:</p> <p>In the event that a delay is not attributable to the Auditor and the project requires an extension with additional man-days to complete the audit, the Bank shall compensate the Auditor for the additional man-days based on the mutually agreed fee structure. In case the applicable fees cannot be mutually concluded, the Bidder shall reserve the right to cancel the Order.</p>	Bidder to comply with RFP terms and conditions.
78	17	Section C	Clause 4	Integration & interfaces	<p>Request the total number of vendors that we would have to consider and also the number of interfaces we would have to review.</p> <p>While we understand the bank will have access to the same. We would need access to interfaces and also would require support from the Bank & Vendor to extract relevant data.</p>	Necessary support will be provided by the Bank
79	17	Section C	Clause 4	To work different vendors and different teams of Bank for the offered assessment	<p>Giving there is clearly a dependency, we would request to add below:</p> <ul style="list-style-type: none"> - Bank is responsible for notification of any 3rd party involvement that may be impacted due to this engagement - Bank will provide a trusted agent to coordinate the involvement of its vendor's team/resources and assist the auditors with the logistics of the engagement including, but not limited to: <ul style="list-style-type: none"> - Scheduling of meetings with various stakeholders - Authorize and supervise active various activities as a part of this project - Assist in collating all supporting artifacts to substantiate compliance status and preservation of audit evidences 	Bidder to comply with RFP terms and conditions.
80	19	Section D	Clause 1.1	Clarification to RFP & Probid queries	<p>Request the bank to have a second round of queries discussion considering there is more information required to adequately arrive at costing and timelines</p>	Bidder to comply with RFP terms and conditions.
81	25	SECTION E - SELECTION OF BIDDER	Clause 3.3	Technical evaluation	<p>Clarity required if the engagement plan is to be submitted along with technical bid. This is contradictory to the earlier mentioned statement of engagement plan in details shall be discussed upon finalization of bidder</p>	Bidder to comply with RFP terms and conditions. Bidder is expected to submit a high-level engagement approach and indicative plan along with the technical bid to demonstrate understanding of the scope, methodology, and timelines.
82	28	Section F	Clause 4	Award of Contract	Numbering to be revisited	Bidder to refer Carrigendum-1
83	28	Section F	Clause 5.3	Award of Contract & Acceptance	Request if the acceptance can be increased to 10 working days instead of 07 days from the date of receipt of order.	Bidder to refer Carrigendum-1
84	29	Section F	Clause 8.1	Performance Security	Request the Performance security be reduced to 3% from TCO and reduce additional claim period to 01 month instead of 02 months	Bidder to refer Carrigendum-1

85	31	Section F	Clause 11.4	Bidder Performance	Definition of satisfactory standards to be captured as part of engagement plan which is to be finalized after discussing with the bank considering the scope	Bidder to refer Corrigendum-1 Bidder to comply with RFP terms and conditions.
86	34	Section G - General Conditions	Clause 4.3	Replacement of Resource	Time period is not specified. Our understanding would be that, this would be discussed as part of initial kick off and agreement would be obtained from the Bank end on acceptable time period	Since the project implementation is time bound in nature, Resources replacement to be done with immediate effect as and when prescribed by Bank.
87	37	Section G - General Conditions	Clause 11.5	Bidder to ensure PII / SPI	Bank will have vendor classification and is there any information with regards to PII / SPI data being handled by each vendor? Providing the same would help us create guard rails while getting information.	Bidder to comply with RFP terms and conditions.
88	37	Section G - General Conditions	Clause 11.6 below	Confidentiality post termination / completeness of contract	Request to have a timeline of 12 months from the completion of the engagement	Bidder to comply with RFP terms and conditions.
89	38	Section G - General Conditions	Clause 13.5	Training and Handholding	Training to be provided to identified spoc's of the bank only twice on the same subject.	Bidder to refer to Corrigendum-1
90	40	Section G - General Conditions	Clause 16	Hiring of Bank Staff	This is a general clause. We would request to limit it to only the team members who are being engaged	Bidder to comply with RFP terms and conditions.
91	40	Section G - General Conditions	Clause 18.2	Location of processing data	These needs clarity as to whether the expectation is the primary place of evaluation and analysis or is it pertaining where the vendor is located? (this will change city to city, Can we mention it as India)	Bidder to comply with RFP terms and conditions.
92	41	Section G - General Conditions	Clause 20 & below	Indemnity	Request if the limit of the indemnity to the contract value?	Bidder to comply with RFP terms and conditions.
93	42	Section G - General Conditions	Clause 21	Conflict of Interest	Request additional time as mentioned earlier for checking Conflict of Interest	Bidder to comply with RFP terms and conditions.
94	56	Annexure - 2 - Pre-Qualification Criteria	Sub point 7	Professionals certificate s	Request to add certifications that include ISO 27001, ISO 22301 and ISO 27701 Request you to reduce the (Min. 10 - CISA, 3 - CISSP, 3 - OSCP should be in pool)	Bidder to comply with RFP terms and conditions.
95	57	Annexure - 2 - Pre-Qualification Criteria	Sub point 11	Turn Over	Request if the turn over requirements be increased to Revenue over INR 50 Crore for each year.	Bidder to comply with RFP terms and conditions.
96	56	Annexure - 9 - Technical Eligibility Criteria			Allow single PO with multiple domain or separate PO for different domain.	The bidder may submit a single Purchase Order covering multiple domains or separate Purchase Orders for individual domains, as applicable.
97	104	Appendix - F	Appendix F	Pre Contract Integrity Pact	* Point of contact from Canara Bank and designation * Should it be left blank or mentioned as per GeM document as Hanumanthu Rao Vanne	Details will be shared with selected bidder. Yes it should be left blank.
98	128	Annexure - 1	Data Processing Terms and Conditions	Annexure number	request Annexure number to be changed - conflicts with Bid Covering Letter	Bidder to refer Corrigendum-1
99	56	Annexure-2 Pre-Qualification Criteria	6	The Bidder should have conducted at least 30 out of 40 (Sub-Domains to be considered) Assessments mentioned under the scope of work in Annexure B, during the last three years as on the submission of Bid in BFSI sector organization/ Scheduled Commercial Banks/ Government Departments/ PSU organization in India.	We kindly request you to consider assessments conducted in Non-BFSI sector organizations as part of the eligibility criteria, in addition to those from BFSI sector organizations, Scheduled Commercial Banks, Government Departments and PSU organizations.	Bidder to refer Corrigendum-1 Bidder to comply with RFP terms and conditions.





100	56	Annexure-2 Pre-Qualification Criteria	6	<p>The Bidder should have conducted at least 30 out of 40 (Sub-Domains to be considered) Assessments mentioned under the scope of work in Annexure 6, during the last three years as on the submission of Bid in BFSI sector organization / Scheduled Commercial Banks / Government Departments / PSU organization in India</p>	<p>We request that the submission of invoices be made non-mandatory. Instead, we propose accepting either the Purchase Order copy or the Engagement Letter as sufficient proof of the assessment conducted.</p>	<p>Bidder to refer Corrigendum-1 Bidder to comply with RFP terms and conditions.</p>
101	56	Annexure-2 Pre-Qualification Criteria	7	<p>The firm should have a pool of at least 50 professionals with valid international accreditation like CISA, CISSP, CISM, CHFI, CEH, OSCP, CCSP, CRISC (Min. 10 - CISA, 6 - CISSP, 3 - OSCP should be in pool) Minimum experience of the professional's post qualification should be 3 years.</p>	<p>We kindly request that the minimum experience requirement of 3 years post qualification for professionals be removed from the eligibility criteria.</p>	<p>Bidder to comply with RFP terms and conditions.</p>
102	83	Annexure-9 Technical Eligibility Criteria	Annexure-9	<p>The bidder has to provide purchase order copy / reference letter in their name from BFSI sector organization / Scheduled Commercial Banks / Government Departments / PSU organization in India duly mentioning the assessment carried out along with Invoice.</p>	<p>We kindly request you to consider assessments conducted in Non-BFSI sector organizations as part of the Technical eligibility criteria, in addition to those from BFSI sector organizations, Scheduled Commercial Banks, Government Departments and PSU organizations.</p>	<p>Bidder to refer Corrigendum-1 Bidder to comply with RFP terms and conditions.</p>
103	83	Annexure-9 Technical Eligibility Criteria	Annexure-9	<p>The bidder has to provide relevant purchase order/ work order / engagement letter along with satisfactory project completion certificate/ Reference letter from the Concerned Organization/Email reference from the client.</p>	<p>We kindly request that the submission of the project completion certificate, reference letter from the concerned organization, or email reference from the client be made non-mandatory. Instead, we propose accepting either the Purchase Order copy or the Engagement Letter as sufficient proof of the assessment conducted. Obtaining project completion certificates or email references from clients for all references can be practically challenging.</p>	<p>Bidder to refer Corrigendum-1.</p>
104	85	Annexure-10 Technical Evaluation Criteria	Annexure-10	<p>The Bidder has to provide purchase order copy / reference Letter in their name from BFSI sector organization / Scheduled Commercial Banks / Government Departments / PSU organization in India duly mentioning the assessment carried out along with Invoice.</p>	<p>We kindly request you to consider assessments conducted in Non-BFSI sector organizations as part of the Technical Evaluation Criteria.</p>	<p>Bidder to refer Corrigendum-1. Bidder to comply with RFP terms and conditions.</p>
105	85	Annexure-10 Technical Evaluation Criteria	Annexure-10	<p>The Bidder has to provide purchase order copy / reference Letter in their name from BFSI sector organization / Scheduled Commercial Banks / Government Departments / PSU organization in India duly mentioning the assessment carried out along with Invoice.</p>	<p>We request that the submission of invoices be made non-mandatory. Instead, we propose accepting either the Purchase Order copy or the Engagement Letter as sufficient proof of the assessment conducted.</p>	<p>Bidder to refer Corrigendum-1. Bidder to comply with RFP terms and conditions.</p>

106	85	Annexure-10 Technical Evaluation Criteria	Annexure-10	The number of domain expert or certified professionals full time employed by the bidder with valid international accreditation like CISA, CISSP, CISM, CHFI, CEH, OSCP, CCSP, CRISC. (Min. 10 - CISA, 6 - CISSP, 3 - OSCP should be in pool) Minimum experience of the professional's post qualification should be 3 years.	We kindly request that the minimum experience requirement of 3 years post qualification for professional be removed from the Technical Evaluation Criteria.	Bidder to refer Corrigendum-1. Bidder to comply with BFP terms and conditions.
107	86	Annexure-10 Technical Evaluation Criteria	Annexure-10	Experience in using Agentix AI for Security Assessment. The bidder must have prior experience in utilizing or demonstrating Agentix AI capabilities in at least one information security assessment within any BFSI sector organization/ Scheduled Commercial Bank/ Government Departments/ PSU organization in India. (The Agentix AI solution should have contributed to improving automation, accuracy, or analytical depth during the assessment).	We kindly request you to consider assessments conducted in Non-BFSI sector organizations as part of experience in using Agentix AI for Security Assessment.	Bidder to refer Corrigendum-1. Bidder to comply with BFP terms and conditions.
108	80	Annexure-8 Scope of Work	Additional Scope of Work	For smooth completion of project, the Bidder should identify one or two of its representatives at Bengaluru as primary point of contact for the Bank.	We understand that either one or two representatives of the Bidder are to be placed onsite at Bengaluru as the primary points of contact for the Bank, while all other project resources may be planned to work remotely for project execution. Kindly confirm if our understanding is correct.	All the resources shall be stationed on prem
109	80	Annexure-8 Scope of Work	Additional Scope of Work	The consultant should deploy the resource for conducting the assessment with relevant Certifications as mentioned in the Annexure - 2 (Sl. No. 7) and having a minimum of 3 years of experience in conducting the same.	Given the diverse nature of the assessment domains listed, we intend to deploy subject matter experts (SMEs) specialized in each domain to ensure high quality and effective assessments. However, the availability of all SMEs holding the specified certifications (CISA, CISSP, CISM, CHFI, CEH, OSCP, CCSP, CRISC) may be limited. Therefore, we request your confirmation to allow the use of domain expert SMEs for conducting assessments even if they do not possess all the mentioned certifications. Kindly confirm if this approach is acceptable.	bidder to comply with BFP terms and conditions.
110	68	Annexure-8 Scope of Work	2	IT Infrastructure & Data Centre Security	Please provide the total number of endpoints in scope, including details on the number of servers, databases, network devices, APIs, and security or monitoring tools currently deployed.	Details will be shared with selected bidder
111	69	Annexure-8 Scope of Work	4	Business Continuity & Disaster Recovery Assessment	Kindly share the total number and physical locations of the Bank's Data Centers and Disaster Recovery sites.	Details will be shared with selected bidder
112	80	Annexure-8 Scope of Work	Coverage of the Assessment	Considering the control points in the above-mentioned domains, the assessment has to be conducted for all the applications of the Bank	Please share the total number of applications currently available across the Bank's IT environment.	Details will be shared with selected bidder
113	78	Annexure-8 Scope of Work	15	AI / ML & Container Security Assessment	Are AI/ML models or containerized platforms currently in use within the Bank's infrastructure? If yes, please specify their scale and the security tools implemented to protect them.	Details will be shared with selected bidder





114	77	Annexure-8 Scope of Work	14.2	Cloud Security Assessment	Are any applications, services, or infrastructure hosted in public cloud environments such as AWS, Azure, or Google Cloud Platform? If so, please provide details on the scope and extent of cloud usage.	Details will be shared with selected bidder
115	General	Annexure-8 Scope of Work	General	General	Will revalidation or follow-up assessments be included as part of the scope of work? If so, please specify the expected timeline or frequency for such revalidation activities.	Bidder to refer RFP terms and conditions.


 DEPUTY GENERAL MANAGER

Place: Bangalore
Date: 10-11-2025

Confidential