केनरा बैंक Canara Bank

Corrigendum-2 to GeM Bid ref: GEM/2025/B/6803799 dated 17/10/2025 for Selection of Cert-In Certified Auditor to Conduct Vendor Risk Assessments along with Due Diligence Audit & Vendor Performance Evaluation of the vendors as on 31/03/2025 and new vendors on an ongoing basis as per Bank Approved matrix in Canara Bank.

It is decided to amend the following in respect of the above RFP:

a. GeM bid document (Bid End date/ Bid Opening Date, Page no. 1 of 7):

Description	Existing details	Amended details
Bid End Date/Time	11/11/2025, 15:00:00	14/11/2025, 15:00:00
Bid opening Date/Time	11/11/2025, 15:30:00	14/11/2025, 15:30:00

b. RFP Document:

Sl No.	Section/Annexure/ Appendix of GeM Bid	Clause No.	Existing Clause	Amended Clause/ New Addition
1.	Annexure-8 Scope of Work	53-Due Diligence on Service Provider 66- IT Security	Existing Annexure-8 Scope of Work	Amended Annexure-8 Scope of Work
2.	Annexure-2 Pre-Qualification Criteria	Point No:8	The Bidder should have Conduct at least one Vendor Risk Assessments /Due Diligence Audit/ Vendor Performance Evaluation in the last five years as on the date of submission of RFP to any Scheduled Commercial Bank.	The Bidder should have Conduct at least one Vendor Risk Assessments /Due Diligence Audit/ Vendor Performance Evaluation in the last five years as on the date of submission of RFP to any Central / State Govt Organization /PSU/ BFSI sector

All the other instructions and terms & conditions of the above RFP shall remain unchanged.

Please take note of the above amendments while submitting your response to the subject RFP.

Date: 06/11/2025
Place: Bengaluru

Deputy General Manager

केनरा बैंक CANARA BANK Tender Processing Section C. P. & V. M. Vertical Technology Services Wing, H.O. Bengaluru-1

Annexure-8
Scope of Work
(Should be submitted on Company's letter head with company seal and signature of the authorized person)

SUB: Selection of Cert-In Certified Auditor to Conduct Vendor Risk Assessments along with Due Diligence Audit & Vendor Performance Evaluation of the Vendors as on 31/03/2025 and New Vendors on an Ongoing Basis as Per Bank Approved Matrix in Canara Bank

Ref: GEM/2025/B/6803799 dated 17/10/2025

Vendor Risk Assessment along with Due Diligence

Vendor Risk Assessment along with Due Diligence involves a structured process of identifying, analyzing, and evaluating potential risks associated with third-party vendors before and during the engagement. This includes comprehensive due diligence to verify the vendor's financial stability, operational capacity, compliance with regulatory requirements, information security and cyber security supply chain risk management measures, Business Continuity Plan / DR Drills and overall risk profile. The objective is to ensure that vendors meet the organization's standards and regulatory guidelines, thereby protecting the organization's operational integrity and minimizing exposure to financial, legal, and reputational risks. This assessment is continuous and risk-based, with more rigorous due diligence applied to higher-risk or critical vendors to safeguard against potential disruptions or compliance failures. The process for carrying out this work is outlined below:

1. **Risk Identification**:

   The risk identification process shall encompass various dimensions, including but not limited to:

   - Data confidentiality and integrity, especially for customer information and sensitive data.
   - Access control mechanisms to safeguard system access and ensure role-based authorizations.
   - Protection of customer and internal data in line with the Bank's Data Protection Policy and relevant data localization mandates.
   - Monitoring the control environment, including internal controls operated by the vendor.
   - Data separation protocols to prevent co-mingling of data among entities or across systems.
   - Incident detection and response procedures, ensuring the vendor complies with timely incident reporting, root cause analysis, and remediation.
   - The gap between the Bank Business Continuity and Disaster Recovery framework in comparison to vendor policy, ensuring continuity of critical processes in the event of disruptions.
   - Check HR and operational policies of vendor, with emphasis on background verification of employee and exit policy of employee, segregation of duties, and conflict of interest avoidance.
   - The Bank's Enterprise Risk Management (ERM) Policy, ensuring the vendor's risks are duly identified, categorized, and mitigated via shared risk frameworks.
   - Cybersecurity supply chain risk management and IT governance practices, including compliance with RBI's expectations for authentication, encryption, patching, and endpoint security.
   - Third-party/sub-contractor risk oversight, if applicable.
   - Further, as per regulatory expectations, including those under RBI's IT Governance Directions, the Bidder must conduct periodic vendor risk assessments and due diligence—annually, semi-annually, or quarterly, depending on the criticality and risk profile of the services provided. These assessments must include reviews of financial stability of vendor, legal compliance, information security posture, business continuity capabilities and audit findings.

केनरा बैंक CANARA BANK Tender Processing Section C.P. & V.M. Vertical Technology Services Wing, H.O. Bengaluru

- All identified gaps and vulnerabilities must be documented, prioritized, and addressed through formal risk mitigation plans, ensuring continual alignment with RBI guidelines and the Bank's internal policies for IT, risk, compliance, procurement, and vendor management.
- Identification and classification of risks associated with the engagement of Third-Party vendors/ services providers of both IT and Non - IT nature.
- The Bidder in consultation with various stake holders/ Verticals/ Wings of the Bank shall diligently identify and assess the potential risks associated with IT/ Non- IT Activity arrangements. This process should encompass various aspects to ensure data confidentiality, access control, customer information protection, control environment monitoring, data separation and incident reporting. All the gaps shall be identified during the Risk Identification process by the Bidder in order to crucially mitigate risks effectively.

2. Risk Capture:

The risk classification must include (but not be limited to) the following broad categories:

2.1 Information Technology (IT) and Infrastructure Risks

Risks related to hardware, network infrastructure, cloud environment, end-of-life assets, version control, and configuration drift. Performance, maintenance and SLA adherence for core and support IT systems.

2.2 Email and Communication Risks

Unsecured email gateways, phishing susceptibility, spoofing risks, and inadequate DLP (Data Loss Prevention) measures. Risks associated with improper encryption and lack of identity protection.

2.3 Information Security/Cyber Security Risks

Lack of compliance with the Bank's Information Security Policy, RBI's baseline cyber security framework, RBI's Master Direction on Outsourcing of Information Technology Services and also cover ISO /IEC 27036-2:2022 standard (ISO/IEC 27036-2:2022 specifies requirements for managing information security risks in supplier and acquirer relationships throughout the entire relationship lifecycle). Gaps in vendor security architecture (e.g., absence of firewalls, endpoint protection, secure data transfer mechanisms).

2.4 Device Risk (Laptops, Mobile Devices, Endpoints)

Insecure or unencrypted endpoints. Absence of Mobile Device Management (MDM), remote wipe policies, or anti-malware on vendor-managed devices.

2.5 Asset and Configuration Management Risks

Weaknesses in asset inventory management, unauthorized software installations, and weak configuration enforcement. Lack of adherence to secure disposal procedures as per RBI norms.

2.6 HR-Related Risks (People Risk)

Risks due to inadequate background verification of vendor personnel. Insider threat vulnerabilities. Non-adherence to minimum staffing levels, skillset gaps, or frequent resource rotation affecting critical operations.

2.7 Facility & Administrative Risk

Physical security controls at vendor premises (e.g., CCTV, access control) not meeting the Bank's or regulatory expectations. Risk of data leakage through physical documentation or E-waste mishandling.

2.8 Privacy and Data Protection Risk

Non-compliance with the Bank's Data Protection Policy, and RBI's guidance on data localization, encryption, classification, and retention. Breach of customer data confidentiality or unauthorized data access by third parties.

2.9 Finance Risk

Vendor financial instability, overdue statutory payments, or pending litigations that may hinder service continuity. Risk of adverse pricing, cost escalations, or force majeure clauses in contracts.

2.10 Compliance & Legal Risk

Non-compliance with RBI and statutory requirements (e.g., Aadhaar Act, IT Act, Companies Act, etc.). Gaps in contract enforceability, absence of audit rights, or ambiguity in SLA definitions. Risk related to compliance with tax and labor laws in India.

2.11 Operational Risk

Service delivery failures, delay in delivery timelines, manpower unavailability, and breakdowns in execution processes. Weak vendor control environment such as lack of process documentation, SOPs, or version control.

2.12 Back-End Processing Risk

Inadequate process standardization in operations performed at the vendor's backend (e.g., data entry, reconciliation, tracking). Manual interventions and lack of maker-checker configurations.

All risk categories must be mapped to relevant controls, mitigation measures, and regulatory compliance obligations (e.g., ISMS controls, SOC reports, audit rights).

The Bidder shall categorize the identified risk in into various above-mentioned categories such as Information Technology, Email, Information Security, Laptop and Mobile Devices, Asset Management, HR, Facility and Admin, Privacy, Finance, Compliance & Legal, Operational, Back End etc.

3. <u>Risk Assessment and Due Diligence Audit:</u>

3.1. The bidder shall assess the severity and probability of each risk to prioritize them based on their potential impact. The Risks identified should be categorized on the basis of the severity such as High, Medium, Low.

3.2. The Bank shall provide a comprehensive and detailed Vendor Risk Assessment and performance evaluation checklist which the Bidder has to consider for each respective Vendor Risk Assessment evaluation. The evaluation will be based on scores to be assigned for different parameters and likewise risk categorization would have to be done by the bidder on the basis of percentage of marks awarded.

3.3. The Risk assessment of vendors shall broadly cover the following key areas ofoperations undertaken by respective vendors:

a. Information Security

b. Information security and cyber security supply chain Risk Management

c. Human Resources

d. User Access/ Application Security

e. Service Level Agreement

f. Business Continuity Plan and Disaster Recovery policy

g. Subcontracting

h. Incident Reporting

i. Awareness and Training

j. IT Outsourcing compliances (applicable for IT Outsourcing Services)

k. Cross - Border Outsourcing

l. Cloud Services Management and Security Considerations

m. Outsourcing of Security Operations Centre

n. Other Points

o. Backup Policy

4. **Concentration Risk Assessment:**

4.1. The bidder in consultation with the various departments/ verticals/ wings of the Bank shall effectively assess the impact of concentration risk, if any, posed by multiple outsourcings to the same vendor/ service provider.

4.2. The Bidder shall find the vendor concentration and the name of the vendor is to be brought to the notice of the Bank and will have to give impartial and effective documented advice regarding further contracts with the particular vendor.

4.3. The selected Bidder shall assist the Bank while onboarding new vendors for different projects/ procurement/ services in avoiding dependency on one or repeated vendors.

5. **Risk Mitigation Strategy:**

5.1. The bidder shall devise and detail the identified Risks and suggest mitigation strategies.

5.2. Suggesting an effective risk mitigation strategy for similar contractual agreements in future that clearly define roles, responsibilities, and performance expectations.

5.3. Evaluate the identified risks based on their likelihood and potential impact by quantifying risks and prioritizing them bases on their Criticality.

5.4. Provide recommendation to Bank/vendors for implementing security measures to protect sensitive data and systems.

5.5. The Bidder shall guide and provide to the risk mitigation strategies to the Bank to analyze and take suitable action plan in response to the identified risks of the vendor.

5.6. The Bidder shall provide recommendation for continuation or discontinuation for the exposed services to avoid risks identified.

Vendor Risk Assessment Scoring Matrix

Sl. No	Baseline Control	Evidence Required	
INFORMATION SECURITY			
1	The Auditor has to verify that the vendor/s is having well defined Information Security Policy/Cyber Security Policy and is reviewed periodically at least once in a year. Auditor has to examine the Documents/Artefacts provided by the Vendor and compare the level of cybersecurity with Bank requirement. 1. Information Asset Management 2. Data Privacy 3. Acceptable usage 4. User Lifecycle &Access Management 5. Human Resource Security 6. IT Operations Security 7. Cryptography 8. Network & Communication Security 9. Application Security 10. Password Management 11. Change Management 12. Security Incident Management 13. Key Management 14. BCP/DR 15. Backup management 16. Anti-Virus Management 17. Patch Management 18. Log Management 19. Physical & Environmental Security 20. Cloud Security 21. cyber security supply chain Risk Management	Vendor IS Policy	
2	Verify the latest information security certifications (like ISO27001 etc.) of vendor organization.	ISO 27001 Certificate	

RISK MANAGEMENT			
3	The bidder shall verify that cyber incidents are reported to the RE by the service provider without undue delay, so that the incident is reported by the RE to the RBI within 6 hours of detection by the TPSP.	Incident Reporting Procedure and corresponding reports	
	The bidder shall identify and monitor the internal and external risks associated with the organization's critical information assets, control processes and security practices of the service provider to disclose security breaches.		
4	Verify the financial status of vendor organization by examining the financial statements and other required documents/artefacts to ensure that the same is adequate to meet the Project/IT Services obligations.	Last two-year balance sheet of Vendor	
	To verify that the Vendor has adhered to the tax structures and taxes levied by Central Government, State Government and local regulatory authorities. Also, confirm if any adverse observations on vendor.	Applicable Tax paid report for last 2 financial years.	
5	To verify whether the vendor is blacklisted or not, by any organization in the last 5 years for any reason.	Background verification of vendor Reports	
	To verify that all relevant reports for the operations/services connected with project is regularly submitted by the vendor.		
6	To verify that whether organization is covered under any Internal and External Inspection.	Inspection Reports	
	To verify the Trade License / Shops and Establishment License of vendors and its validity period.	Licence	
7	To verify that vendor has obtained prior consent of Bank before sub-contracting to the third party, if any	Agreement	
	To verify the capabilities of vendor to ensure that applications and system services developed, or enhanced, to handle Bank Information, prudent information security measures throughout the entire development process.	Application Development Policy and last year any Application developed full cycle report	
8	To verify that the vendors are conducting regular testing of products/ application/ solution provided to the Bank	DR Drills / Other Audit Reports	

केनरा बैंक CANARA BANK Tender Processing Section C. P. & V. M. Vertical Technology Services Wing, H.O., Bengaluru

HUMAN RESOURCES			
9	Does the vendor organization perform appropriate background verification and criminal checks through Police verification for employees?	Police verification/ Back ground verification of employees.	
10	To verify that vendors are providing the details of employees deployed for the Bank's project with proper due diligence including educational /technical qualification/training required for the respective projects.	Email and details of training and qualification and Experience of the employee	
11	To verify the Vendor's HR Policy and ascertain that it as per the required guidelines adopted by the Vendor's Organization.	HR Policy of Vendor	
12	To verify whether the vendor is having any industrial relation problems and report, if any	IR Policy of Vendor	
13	Does the Vendor have a documented Code of Business Ethics and Conduct ("COBEC") / Anti-Bribery and Anti-Corruption ("ABAC") policies for employees?	Code of Business Ethics and Conduct ("COBEC") / Anti-Bribery and Anti-Corruption ("ABAC") policies	
14	To ascertain that vendor are having a formal disciplinary process in place for employees who have violated organizational security policies and procedures.	HR Policy of Vendor	
15	To verify that vendor is complying with guidelines and regulation under Digital Data Protection Act 2023 & approved data protection and privacy policy covering all aspects of personal data collections, storage including permissible data types, retention, restriction of usage, destruction, breach handling, etc.	Policy on Digital Data Protection Act 2023.	
16	Does the vendor have a mechanism to classify & protect Bank related data. (Refer Information Classification Policy) E.g., Confidential/Restricted/Public	Information Classification Policy	

17	To verify the vendor performs Security checks to ensure the data file residing in the vendor server/ local computers are secure from external threats & data is secured for data at rest/ storage and of data at flow.	Secure Configuration Review/ encryption used to safeguard data file residing in the vendor server/ local computers. Data Classification Policy	
18	To verify whether the data shared to the vendor is classified by the Bank and stored within the Bank or with the vendor	Data Classification Policy	
19	To verify that the vendor is using licensed software. Also confirm that firewall and anti-virus software used are licenses and latest.	List of Licensed software used Details of Firewall & Antivirus solution used	
20	To review/ verify the Network / Database / Source code review of Application / dataflow Architecture of vendors and also ascertain the periodicity of its review for any drawback	Network Architecture Review report Application / Database Hardening document Data Flow diagram of Application used	
21	To verify/review the security of vendor's network devices/application/OS and databases	AMC	
22	Whether the vendor has Intrusion Detection System/ Intrusion Prevention System (IDS/IPS) implemented in the environment?	Firewall Configuration	

केनरा बैंक CANARA BANK Tender Processing Section C. P. & V. M. Vertical Technology Services Wing, H.O. Bengaluru

23	To confirm the availability of email security E.g. SPF, DMARC etc. is in place.	E-mail configuration report for SPF & DMARC	
24	To verify if vendor is conducting periodical review of User Access Management.	User Access Review	
25	To verify that the service provider staff is not having any access to customer information	User Access need to be check	
26	To verify if there is a centralized system for log monitoring and analysis of Database activities and commands performed, collected and analysed by the DBA team, and if logs are being reviewed periodically (Daily/Weekly/Quarterly) by the security team and Quarterly by the CISO/IT-IS Heads Whether all logs are being shared with SIEM and DAM.	Log register	
27	To verify if the edit access to log file blocked for users / privileged users as well as admins / super admins?	Privilege access management configuration	
28	To verify that vendor has provided access to all books, records and information relevant to the outsourced activities contracted with them.	Access control	
29	To verify the controls to ensure customer data confidentiality and service provider liability in case of breach of security and leakage of confidential customer related information.	Access control	
30	To verify that vendor has implemented centralized authentication and authorization system for accessing and administering applications, operating systems, databases, network and security devices/systems, point of connectivity (local/remote, etc.) including enforcement of strong password policy, two-factor/multi-factor authentication depending on risk assessment and following the principle of least privileges and separation of duties	Password Policy	
31	To verify that the vendors have baseline security requirements / configurations to all categories of devices (endpoints / workstations, mobile devices, operating systems, databases, applications, network devices, security devices, security systems, etc.), throughout the lifecycle (from conception to deployment) and carry out reviews periodically.	Secure Configuration Document / Last configuration Audit report for all Network Devices (endpoints /	

Canara Bank Tender Processing Section C. P. & V. M. Vertical Technology Services Wing, HO

		workstations, mobile devices, operating systems, databases, applications, network devices, security devices, security etc..)	
32	To verify that vendor has implemented the risk-based transaction monitoring or surveillance process as part of fraud risk management system, as per requirement of the services provided or project handled by them	Fraud Risk Management and last one-year report	
BUSINESS CONTINUITY PLAN AND DISASTER RECOVERY PLAN			
33	REs shall require their service providers to develop and establish a robust framework for documenting, maintaining and testing Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) commensurate with the nature and scope of the outsourced activity as per extant instructions issued by RBI from time to time on BCP/ DR requirements.	BCP Plan DR Drill Report	
34	REs shall ensure that service providers are able to isolate the REs' information, documents and records and other assets.	Review in case cloud providers are used.	
35	Impact on Bank's business operations in case the activity to be outsourced gets disrupted or compromised		
36	Impact on customers of the Bank in case the activity to be outsourced gets disrupted or compromised		
37	To verify that the vendor has adequate mechanism to provide uninterrupted technical operations and services, especially during transitions, upgrades or unexpected events and ensure that systems, data and processes remain available, reliable and secure.	Manpower/ Process to provide uninterrupted technical operations and services, especially during transitions, upgrades or	

		unexpected events	
38	To verify that the Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) maintained and tested on regular basis. Also confirm the periodicity of testing. Related Documents and Artefacts provided by the vendors to be verified.	BCP/DR Plan	
39	Whether the Wing is having the alternate vendors on backup for resuming the activity in case of disruption and the level of difficulty in replacing the vendor.	Change Management process & last one-year change report	
40	To know the location of backup media storage and to verify whether there a secure process for onsite & offsite backup media protection during storage pertaining to Bank operations and to verify whether Backup data /files / devices be encrypted with latest security standards (AES 256 etc.).		
41	To verify whether the data shared to the vendor is classified by the Bank and stored within the Bank or with the vendor and does the vendor have defined retention period of Bank data (if stored with vendor)		
42	To verify that vendor has the capabilities to handle changes to business applications, supporting technology, service components and facilities should be managed using robust configuration management processes, configuration baseline that ensure integrity of any changes thereto		
SUBCONTRACTING			
43	Wherever Subcontracting is allowed to the Vendor for the services / project provided to Bank, whether the due diligence processes are followed for evaluating subcontractors and are complying with the same standards/requirements as primary vendors.	SLA	
44	To verify that the Security prescriptions of the Subcontractor are equivalent to those of primary Vendor.	Security prescriptions of the Subcontractor if sub-contracting has been done	

केनरा बैंक CANARA BANK Tender Processing Section C. P. & V. M. Vertical Technology Services Wing, H.O., Bengaluru

INCIDENT MANAGEMENT AND REPORTING			
45	To verify that the vendors have incident management plan with adequate mechanism for identify, classify, and respond to incidents involving Projects.	Last one-year Incident Report Incident management plan	
46	To check whether vendors have a set of procedures are in place for notifying user groups about significant incidents.	Incident management report	
47	To check if the root cause analysis is performed for the security incidents.	RCA report	
48	To verify whether vendor conduct post-incident reviews to identify lessons learned and areas for improvement.	Last one-year Incident Report, No RCA, ask KYNDRL	
GRIVENCE REDRESSAL MECHANISM			
49	To verify that vendor has a risk management module.	Risk Management policy	
50	To verify whether the vendor have a documented policy to classify customer interactions into request/query/compliant		
51	To verify if there is a four-eye principle to record/resolve/report customer complaints		
52	To verify the policy and supporting procedure for safeguard of client Intellectual Property		
DUE DILIGENCE ON SERVICE PROVIDER			
53	a) Financial soundness and ability to service commitments even under adverse conditions b) Business reputation and culture, compliance, complaints and outstanding or potential litigations conflict of interest, if any c) External factors like political, economic, social and legal environment of the jurisdiction in which the service provider operates and other events that may impact data security and service performance d) Details of the technology, infrastructure stability, security and internal control, audit coverage, reporting and monitoring procedures, data backup arrangements, business continuity management and disaster recovery plan e) Capability to identify and segregate REs data f) Quality of due diligence exercised by the service provider with respect to its employees and sub-contractors		

	g) Capability to comply with the regulatory and legal requirements of the Outsourcing of IT Services arrangement h) Information/ cyber security risk assessment i) Ensuring that appropriate controls, assurance requirements and possible contractual arrangements are in place to ensure data protection and RE's access to the data which is processed, managed or stored by the service provider j) Sub-contractor in this Master Direction refers only to those providing material / significant IT services to the TPSP specific to the material IT Services arrangement that the RE has entered into with the TPSP. k) Ability to effectively service all the customers while maintaining confidentiality, especially where a service provider has exposure to multiple entities **l) <u>Aggregate exposure to a particular service provider.</u>** **m) <u>Existing Performance/Past Experience.</u>** **n) <u>Previous Successful Implementation of the projects in peer Banks</u>**		
OUTSOURCING AGREEMENT			
54	The agreement at a minimum should include (as applicable to the scope of Outsourcing of IT Services) the following aspects: a) Sub-contractors b) Effective access by the RE to all data, books, records, information, logs, alerts and business premises relevant to the outsourced activity. c) Regular monitoring and assessment of the service provider by the RE for continuous management of the risks holistically. d) Type of material adverse events (e.g., data breaches, denial of service, service unavailability, etc.) and the incidents required to be reported to RE to enable RE to take prompt risk mitigation measures. e) Service-Level Agreements (SLAs) formalizing performance criteria to measure the quality and quantity of service levels. f) Storage of data g) The service provider to provide details of data (related to RE and its customers) captured, processed and stored. h) Types of data/ information that the service provider (vendor) is permitted to share with RE's customer i) Contingency plan(s) to ensure business continuity and testing requirements j) Right to conduct audit of the service provider, is the backup of audit trail maintained and is it maintained on a centralized server k) Right to seek information from the service provider about the third parties l) Prior approval/ consent of the RE for use of sub-contractors by the service provider for all or part of an outsourced activity		
55	To verify that the service level agreement is executed as per Purchase Order terms. All the regulatory and Bank/project Specific clauses are included in the Service Level Agreement.	PO & SLA	

56	To verify Confidentiality or Non-Disclosure Agreement (NDA) for protection of information is executed by the vendor.	Non-Disclosure Agreement	
57	To verify the source codes are deposited by the Vendor wherever Escrow arrangement is stipulated in the Purchase Order.	Escrow Agreement	
EXIT STRATEGY			
58	To verify whether the vendor has proper exit process		
59	To verify whether there is a structured process with defined responsibilities for removal of access rights & revoking of assets when person leaves Bank scope of work		
PHYSICAL SECURITY			
60	To Verify physical and environmental security measures in place like CCTV, Fire extinguisher, fire alarm, Smoke detector, biometric, UPS, AC, etc.	Physical Security Review Report	
61	To verify if the vendor performs mock drills at the regular intervals.	Mock Drill Report	
CAPACITY MANAGEMENT			
62	To verify whether vendor has the approved process for managing the size, amount, load and scalability of information systems and resources.	Capacity Management Plan	
63	To verify that vendor has the approved process of ongoing monitoring to detect capacity limits and suitable tools to support capacity management activities	Capacity Management Plan	
64	To verify whether the Wing has capability to bring the activity in house in case of disruption		
CLOUD SECURITY			
65	To verify whether vendor perform cloud-based data segregation and separation between client data and other customer data and comment on security and governance measures in place for cloud services, including aspects such as service and technology architecture, identity and access management, security controls, monitoring, and disaster recovery preparedness		

IT SECURITY			
66	**To verify whether the service provider is using separate physical/logical environments for systems development, testing, staging and production for robust IT infrastructure as per PO/RFP/SLA terms wherever applicable.**		
CHANGE MANAGEMENT			
67	Does the vendor have a documented procedure for identifying the changes to be notified to the Bank, approval for the same, and communication process, if needed?		
SERVICE DELIVERY			
68	Comment on contractual document with Bank on following: -Scope -Performance standards -Access to books, records -Right to inspect & audit -Confidentiality & Security -Termination clause - Business Continuity -Dispute resolution -Applicable laws & regulatory guidelines -Subcontracting -Information security clauses - Indemnity clause - obligation of the service provider - Publicity & proprietary rights - Insurance		

OTHER CONTROLS			
69	Whether the vendor performs vulnerability checks to ensure the data file residing in the vendor server/ local computers are secure from external threats		
70	Whether the fact that the vendor can use sub-contractor is mentioned in the agreement and responsibilities of the sub-contractor/ vendors towards the Bank are clearly articulated in the agreement.		
71	Number of activities already outsourced to the vendor (for nil activity- Low, for up to 5 activity- Medium and for more than 5 activity- high)		
72	Check validity of the insurance coverage and adequacy of coverage.		
73	All servers are integrated with SIEM for monitoring.		
74	All servers are integrated with Privileged Identity Management Solution (PIMS) for access by privileged identities.		
75	All Database servers are integrated with Database Access Monitoring (DAM) solution.		

6. **Due diligence shall take into consideration below key areas:**

   a. Qualitative, quantitative, financial, operational, legal and reputational factors.

   b. Risks arising from concentration of outsourcing arrangements with a single or a few services provider/s.

   c. Past experience and demonstrated competence to implement and support the proposed IT activity over the contract period;

   d. Financial soundness and ability to service commitments even under adverse conditions;

   e. Business reputation and culture, compliance, complaints and outstanding or potential litigations;

   f. Conflict of interest, if any;

   g. External factors like political, economic, social and legal environment of the jurisdiction in which the service provider operates and other events that may impact data security and service performance;

   h. Details of the technology, infrastructure stability, security and internal control, audit coverage, reporting and monitoring procedures, data backup arrangements, business continuity management and disaster recovery plan;

   i. Capability to identify and segregate Banks data;

   j. Quality of due diligence exercised by the service provider with respect to its employees and sub-contractors;

   k. Capability to comply with the regulatory and legal requirements of the Outsourcing of IT Services arrangement;

   l. Information/ cyber security risk assessment;

   The Bidder shall conduct vendor risk assessment and due diligence on the basis of above-mentioned criteria and Metrix mentioned as under and regulatory requirement as per industry standard and document the risk assessments and obtain necessary approvals from the authorized Bank personnel.

The bidder shall share the findings list with vendor SPOC and coordinate with the Bank to share the risk remediation plan.

Vendor Performance Evaluation

The selected vendor shall, in order to establish a continuous evaluation strategy for vendor performance that enhances delivery quality, ensures accountability, and mitigates concentration risk by assessing vendors at the project level and aggregating their performance at the vendor level. Vendor performance to be measured based on the following predefine Matrix, which is mentioned as under.

Vendor Performance matrix			
Sl. No.	**Parameter**	**Maximum marks**	**Weightage**
Financial Stability:		**20 Marks**	**20**
1.	Assessment of previous year balance sheet of vendor	**5**	**3.33**
2.	Positive Net worth	**5**	**3.33**
3.	Profitability	**5**	**3.33**
4.	Erosion in net worth in last three year shall not be more than 30%	**5**	**3.33**
5.	Constitution of the vendor/ or any change reported in the management during the services	**5**	**3.33**
6.	Market Share of the particular services taken from the vendor (Include Peer Bank feedback also)	**5**	**3.33**
Operational performance:		**50 Marks**	**50**
1.	Compliance to scope of work	**5**	**2.09**
2.	Adherence /Breach to SLA terms	**5**	**2.09**
3.	Uptime	**5**	**2.09**
4.	Quality of resources	**5**	**2.09**
5.	Availability of resources	**5**	**2.09**
6.	Continuity of resources	**5**	**2.09**
7.	Adherence of delivery/project timeline	**5**	**2.09**
8.	Performance of the Solutions/ Project	**5**	**2.09**
9.	No. of incidents/ issues	**5**	**2.08**
10.	TAT/MTTR	**5**	**2.08**
11.	Response time	**5**	**2.08**
12.	Effectiveness of escalation matrix	**5**	**2.08**
13.	Ease of Modification/ customization/Change Request	**5**	**2.08**
14.	Quality of Service	**5**	**2.08**

15.	Failure/Lapses occurred during the services, resulting financial and reputational loss to the Bank.	5	2.08
16.	DR readiness & testing	5	2.08
17.	Updated SOP & Manual	5	2.08
18.	Adhering to RTO & RPO	5	2.08
19.	Patch/ version updates/ upgrade	5	2.08
20.	Automation and use of AI	5	2.08
21.	VAPT-remediation TAT	5	2.08
22.	Training plan	5	2.08
23.	Adhering to DPDP	5	2.08
24.	Delivery of items card, cheque book, welcome kit etc. to end users	5	2.08
Regulatory/Statutory Compliance:		**30 Marks**	30
1.	DR availability in case of OPEX model	5	3.35
2.	Compliance to BCP Standards	5	3.35
3.	Compliance to Outsourcing	5	3.35
4.	Compliance to DPDP guidelines	5	3.35
5.	Compliance to Cyber Security guidelines	5	3.35
6.	Adherence with ICT policy	5	3.35
7.	Compliance to other statutory guideline relevant to scope of work	5	3.30
8.	Escrow arrangement	5	3.30
9.	Timely execution of SLA/ MSA agreement	5	3.30

The weightage will be decided on maximum marks achieved for each Parameter and same will be **rated on a scale of 1 to 5**, where:

- **5 = Excellent** (Exceeds expectations significantly)
- **4 = Good (Meets expectations with minor improvements needed)**
- **3 = Average (Meets minimum expectations)**
- **2 = Below Average (Performance issues observed)**
- **1 = Poor (Major deficiencies or SLA breaches)**

Each vendor will be evaluated on the basis of above matrix, accordingly scoring will be done.

7. **General requirement from the Bidder:**

7.1. Selected bidder has to ensure comprehensive assessment of parameters such as classification of vendor into Low, Medium & High Risk as per Bank rating model and readiness to DPDP act and related latest regulatory guidelines.

7.2. Selected bidder has to ensure 360-degree evaluation by the empanel auditor covering both technical, governance and banking aspect.

Tender Processing Section C. P. & V. M. Vertical

7.3. Collection of evidences/ artefacts from respective vendors and User Groups within the Bank for drafting the Audit report. The Bidder shall have to coordinate and follow up with respective vendors and User groups of the Bank for data collection for providing draft reports of Vendor Risk Assessment and Due Diligence along with performance evaluation audit report.

7.4. The bidder shall submit signed final Vendor Risk Assessment and Due Diligence audit reports along with performance evaluation audit report, their respective Risk Ratings in format mutually agreed by the Bank.

7.5. The Bidder shall suggest the required artifact or action for mitigation and closing the Audit observations as per Risk Mitigation Strategy of the IT Services Outsourcing Policy of the Bank.

7.6. The bidder shall ensure compliance to all the regulatory frameworks and guidelines regarding Vendor Risk Assessment and due diligence issued by regulatory authorities from time to time and related Policies of the Bank. Some of the key Guidelines/ Instruction issued by Govt./ Regulatory authority & Policies of Bank are as under:

a) RBI Master Direction on Outsourcing of Information Technology Services vide Ref No- RBI/2023-24/102 DoS.CO.CSITEG/SEC.1/31.01.015/2023-24 Dated- 10.04.2023.
b) RBI Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices vide Ref No - RBI/2023-24/107 DoS.CO.CSITEG/SEC.7/31.01.015/2023-24 Dated - 07.11.2023.
c) The Digital Personal Data Protection Act, 2023.
d) Bank's IT outsourcing Policy and Procurement Policy.
e) Compliance towards various internal policy and frameworks of the Bank such as Information Security, Cloud Adoption Policy, IT Services Outsourcing Policy, BCMS and BCP framework policy etc. of the Bank.
f) Any other related Directions and frameworks that the Regulatory agencies may introduce in future.

Note: The above list is inclusive and not exhaustive i.e., Terms of reference shall include providing professional assistance for all activities required for the implementation for the Vendor Risk Assessment and Due Diligence Audit. The terms of reference shall also include implementation of the guidelines/ recommendations/ instructions of the Reserve Bank of India/ Ministry of Corporate Affairs/ Indian Banks Association/ Institute of Chartered Accountants of India or any other statutory/ non-statutory regulatory authority issued or to be issued during the contract period, to the satisfaction of the Bank without any additional cost.

We confirm that the information furnished above is true and correct. We also note that, if there are any inconsistencies in the information furnished above, the bid is liable for rejection. All documentary evidence/ certificates confirming compliance to Scope of Work should be part of Technical cum Eligibility.

Note: Quality of report should be at part with industry standard and comply with regulatory requirement.

We comply with the above Scope of Work; Non-compliance to any of the scope of work will lead to disqualification in Technical proposal.

Date:
Place:

Signature with seal
Name:
Designation:

केनरा बैंक CANARA BANK Tender Processing Section C. P. & V. M. Vertical Technology Services Wing, H.O. Bengaluru