केनरा बैंक Canara Bank

Corrigendum-2 to GEM/2025/B/5787764 dated 06/01/2025 for Selection of vendor for end to end implementation and maintenance of comprehensive centralized Early Warning Signal EWS Solution for a period of five years in Canara Bank.

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

Sl. No.	Section/ Annexure/ Appendix of GeM Bid	Clause No.	Existing Clause	Amended Clause
1.	Section B-Introduction	8.Scope of Work	For smooth completion of project, the selected bidder should identify one or two of its representatives each at Bangalore and Mumbai as a single point of contact for the Bank.	For smooth completion of project, the selected bidder should identify one or two of its representatives at **Hyderabad** as a single point of contact for the Bank. It applies for both **Pre & Post Go-Live.**
2.	Section C - Deliverable and Service Level Agreements	1.Project Timelines	Existing Project Timelines	**Amended Project Timelines attached along with this Corrigendum.**
3.	Section C - Deliverable and Service Level Agreements	3.Security	3.9 The selected bidder will have to establish all the necessary procedures/ infrastructure/ technology/ personnel to ensure the Information System Security as per the guidelines prescribed by RBI and the policies of the	3.9 The selected bidder will have to establish all the necessary procedures/infrastructure/technology /personnel to ensure the Information System Security as per the guidelines prescribed by RBI and the policies of the **Bank.**
4.	Section C - Deliverable and Service Level Agreements	8.Payment Terms	External Data cost Payment shall be made half yearly in arrears for the number of accounts as per the log reports/ audit trail report submitted to the bank.	External Data cost Payment shall be made **quarterly** in arrears for the number of accounts as per the log reports/ audit trail report submitted to the bank.
5.	Annexure-2	Pre-Qualification Criteria	The proposed EWS solution should have been implemented in at least One Scheduled Commercial Bank in India as on RFP date. The Bidder has to submit Purchase Order/Work order/contract agreement along with along with satisfactory project completion certificate/ Reference letter from the Client.	The proposed EWS solution should have been implemented in at least One Scheduled Commercial Bank in India as on RFP date. The Bidder has to submit Purchase Order/Work order/contract agreement along with satisfactory project completion certificate/ Reference letter from the Client to confirm this from **bidder/OEM.**

6.	Annexure-8	Scope of Work	25. The vendor will have to supply and install the solution at the Bank's Data Centre in Bangalore and also should replicate at Disaster Recovery Site, Mumbai/ other major city in India. The DC will be with high availability and DR without high availability. DC and DR will function as Active/Passive.	25. The vendor will have to supply and install the solution at the Bank's Data Centre in Bangalore and also should replicate at Disaster Recovery Site, Mumbai/ other major city in India. **All the Hardware within the DC and DR shall have redundant components in Active-Active or Active-Passive mode to ensure high availability at each site**. DC and DR will function as Active/Passive.
7.	Annexure-8	Scope of Work	XIX. Core banking system (CBS): The bank has envisaged upgrading the CBS in near future. Presently Bank is having Flexcube. Bidder has to take it into account while bidding. Solution should work in upgraded versions as and when implemented by Bank & no extra cost will be paid towards the same. The bidder is to propose the mandatory interfacing cost from M/S Flexcube (CORE Banking Solution partner of the bank) as part of the bidder's commercial offering in the Commercial.	**This clause stands deleted.**
8.	Annexure-8	Scope of Work	At any point of time during the contract period, the resource utilization like CPU, Memory, Database etc. should not exceed 60 % of the total capacity. The selected bidder shall provide any additional hardware without any additional cost to the bank, to maintain the aforesaid performance parameter for the entire contract period.	**At any point of time during the contract period, the resource utilization should not exceed the defined Average Threshold of alloted capacity as per the details below.** **Average CPU Threshold: 70%(Utlized)** **Average Memory Threshold: 85%(Utlized)** **Average Storage Space Threshold: 85% (Utilized) or minimum 10GB free.** **Average shall be calculated by considering values in hours (1 to 24) / Business Hours.** The selected bidder shall provide additional hardware if required, without any additional cost to the bank, to maintain the aforesaid performance parameter for the entire contract period.

9.	Annexure-8	Scope of Work	11. License and Hardware Sizing:	11. License and Hardware Sizing: New Clause: **11.9. Number of Transactions approx. 3 lakhs per day.**
10.	Annexure-9	Functional and Technical Requirements	Existing Annexure-9 Functional and Technical Requirements	**Amended Annexure-9 Functional and Technical Requirements attached with this Corrigendum**
11.	Annexure-10	Technical Evaluation Criteria	Existing Annexure-10 Technical Evaluation Criteria	**Amended Annexure-10 Technical Evaluation Criteria attached with this Corrigendum**
12.	Appendix-G	Draft Contract Agreement	Existing Draft Contract Agreement	**Amended Draft Contract Agreement attached with this Corrigendum**

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

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

Date: 29/01/2025
Place: Bengaluru

Deputy General Manager

Tender Processing Section

Amended Annexure-9

Functional and Technical Requirements

Should be submitted on Company's letter head with company seal and signature of the authorized person)

SUB: Selection of vendor for end-to-end implementation and maintenance of comprehensive centralized Early Warning Signal (EWS) Solution for a period of five years in Canara Bank.

Ref: GEM/2025/B/5787764 dated 06/01/2025.

Note:	
(a)	The specifications of proposed EWS system/ solution are detailed below. These specifications are only indicative but not exhaustive.
(b)	If the bidder feels that certain features offered are superior to what has been specified by the Bank, it shall be highlighted separately. Information regarding any modification required in the proposed solution to meet the intent of the specifications and state-of-the-art technology shall be provided. However, the Bank reserves the right to adopt the modifications/ superior features suggested/ offered.
(c)	The bidder shall provide all other required equipment's and/or services, whether or not explicitly mentioned in this GeM bid, to ensure the intent of specification, completeness, operability, maintainability and upgradability.
(d)	The bidder shall own the responsibility to demonstrate that the solution offered are as per the specification/performance stipulated in this GeM bid and as committed by the bidder either at site or in bidder's work site without any extra cost to the Bank.

The bidder should provide their response to the Technical and Functional Requirements by giving the compliance level as explained below. Explanations/ suggestions of the bidder against each requirement should be given in the Remarks column. If more explanation of a point is needed, documents can be attached to Remarks Column of the respective requirement.

1) Functional and Technical Requirements

a. Mandatory (Essential) Requirements

Sl No	Technical and Functional Requirements	Compliance Yes/No	Remarks
A	Functional Overview		
a	The proposed solution should support integration with both internal and external data sources and capable of capturing/ consumption of data from any other package for generation of EWS alerts.		
b	The triggered data-based alerts frequency should be Real time/ Near real time/ Daily/ Monthly/ Quarterly/ Half-Yearly/ Yearly are available to the users without any time gap.		
c	System must handle expected data loads and allow for future expansion. Ensures high availability and reliability.		

Sl No	Technical and Functional Requirements	Compliance Yes/No	Remarks
d	Rule engine that provides facility of configurable analytical routines to analyze data and serve as input for alerts and ensures accuracy of the alerts with reliability and precision.		
e	The proposed solution capable of alerting admin users of failed extraction jobs so that the same can be triggered at the earliest without loss of data		
f	Integration between EFRM System, AML System and other modules for case management for reporting purposes.		
g	The existing legacy data in the existing solution should be migrated to new solution without any obstacles, loss or deviation and must be complete in nature.		
B	**Transaction Monitoring**		
1	**Data Integration Capabilities: Internal Data Systems:**		
a	The proposed solution must have integration capabilities from a variety of sources, like Core Banking system, Loan Origination Systems, Rating systems, Audit Systems, KYC and AML systems, LCM, Internal black list databases, BI systems & Data ware houses, HRM systems, etc.,		
b	Store rules/ transactional/ alert/ reports data securely in a centralized data repository which can help to clean, standardize, match and enhance data as it moves into the master reference file and is reused for downstream processes.		
c	Customized branch, RO and CO level data entry screens to be provided as part of application to capture data from all the units.		
d	Implement appropriate access controls and encryption mechanisms to safeguard sensitive data.		
e	Utilize advanced algorithms to perform fuzzy logics for variations in spellings, transliterations, and phonetic similarities and cleanse and normalize data to remove inconsistencies and errors like scenarios.		
f	Transform data into a unified format for analysis, including standardizing date and time formats, currency codes, and other relevant data points.		

2	**Text Mining:**		
a	The proposed solution must have a utility capable of visualizing and extracting (text-mining) information relevant for the alerts from internal documents (such as stock audit reports, inspection reports, annual reports).		
b	The text mining utility should have capability to read the document (PDF, JPG) and generate alerts (i.e., OCR capabilities)		
c	EWSS must have text mining analytics for analysing negative news/ sentiment from news aggregators like Bloomberg and other agencies (e.g. Tax/Excise raids/ penalties, Regulator action suits, Loss of large contracts etc.)		
d	EWSS must have text mining analytics capability for analysing negative news/sentiment from regulators sites (e.g., SEBI, BSE, and NSE etc.).		
3	**Web Harvesting:**		
a	The system should have web harvesting capabilities to search for news items, articles etc. relevant for the purpose of alert generation.		
b	The web harvesting application should be capable of integrating to feeds business/news/security exchange/social websites from various (based on a schedule).		
c	The application should have capabilities to read from the XML files.		
c	Should contain crawling capabilities which should be able to retrieve Web pages that go many layers deep originating from a specific URL. (Required websites & Subscription for which will be provided by the Bank).		
d	The above referred pre-existing library should be configurable for addition/deletion/modification of keywords/phrases.		
e	The internet scanning utility should facility to configure list of company/ borrower names, directors/ Key Managerial Personnel names etc.		
4	**EWS Rules and Analytical Capabilities:**		
a	The EWS must have facility to identify the entities in which the Directors holds the position on the basis of DIN (based MCA data).		
b	EWSS must provide an option where performance profiling of entities can be done on financial parameters (e.g., Financial Ratios, business growth trends etc.) which can be saved as templates that can be specific to an entity or an industry.		
c	EWSS must provide an option for template where performance profiting of entities can be matched against peers and industry averages (for a multitude' of parameters).		
d	EWSS must provide with the flexibility to write bank's own rules that trigger early red flags against borrowers.		

e	EWSS should generate alerts on all early warning signals scenarios suggested by RBI/ DFS/ Bank.		
f	EWS solution should carry out intelligent Fact's extraction regarding these accounts by identifying and filtering irrelevant news items and keeping only relevant news items.		
g	EWSS should not just administer rules looking for risk patterns in unstructured data, but also automatically discover new rules which explain a particular risk attribute for the account.		
h	Management Risk indicators like resignation of the key personnel and frequent changes in the management.		
i	Business risk indicators like labour unrest in borrower's company.		
j	EWSS should automatically provide the score for the alerts for early warning indicators.		
k	Rules engine should have the ability for each transaction to be evaluated by every rule.		
l	Rules engine should be able to identify the rules triggered by a transaction.		
m	Rules engine should be able to list, by priority, of all rules triggered by a transaction.		
n	EWSS must provide a framework for deciding what thresholds of business rules will result in an alert. The thresholds may be: Quality based, Event based, Industry based or combination of the above.		
o	EWSS must permit an option for creation of a manual alert for non-standard events that cannot be ordinarily captured by the EWSS.		
p	The proposed solution should contain a sophisticated and GUI based predictive modelling and analytical workbench.		
q	The proposed solution should enable identification of suspicious borrowers through a judicious mix of anomaly detection, business rules, predictive modelling and network analytics.		
r	The proposed solution should help analysts to visualize complex network of relationships between entities - such as people, organizations, places/ locations, things and events over time and across multiple dimensions.		
s	The proposed solution should have in-built modules for analysis of variance, multivariate analysis and statistical algorithms to build prediction models such as Linear, Logistic, Non-Linear and Quantile regression models, Generalized Linear models, Predictive partial least squares and Decision trees.		
t	The proposed solution should have in-built modules for Unsupervised learning with cluster analysis and mixed variable clustering.		
u	Automatically generate alerts for transactions that match predefined rules, scenarios, or anomalies.		

CANARA BANK Tender Processing Section

v	Develop scenarios that encompass various transaction attributes, such as transaction amount, frequency, source, destination, customer remarks/ narration and more.		
w	Regularly review and update rule sets, scenarios, and models based on emerging risks and regulatory changes.		
5	**Workflow Management:**		
a	Implement a workflow system to manage the investigation process for flagged alerts.		
b	Define roles and responsibilities for reviewing, escalating, and resolving alerts with permissions to access, edit, approve, close or escalate cases at various workflow stages.		
c	Based on result of the alert triggers, EWS must provide a framework for converting alerts that need deeper analysis or actions.		
d	EWS must provide facilities to attach documents to the case.		
e	EWS solution should have the ability to assign activities in the workflow to a group of users.		
f	The user should have ability to write notes in the cases.		
g	Provide a complete audit trail of actions within each workflow, including case handlers, timestamps, and actions taken, for compliance and accountability.		
6	**Alert Generation Module:**		
a	EWS must provide a framework for deciding what thresholds of business rules will result in an alert. The thresholds may be: Amount based (absolute or % of limit), Count based, Quantity based, Industry based, or combination of above.		
b	EWS must permit an option for creation of a manual alert for non-standard events that cannot be ordinarily captured by the EWS.		
c	EWS should have capability to group alerts into single entity actionable events.		
d	EWS have ability for automatic assignment of cases to investigators, ability for supervisor to override and assign cases manually in case of need.		
e	Providing workspace for RFA Committee: Ability to add remarks, add attachments, mark committee's decision and confirm remedial action, facilitated by analytics on cases being investigated.		
7	**Alert Scoring:**		
a	The EWS is expected to have features for scoring alerts based on suitable formulae.		
b	The EWS is also expected to have framework that assigns provide an overall risk score to each loan account and overall, at a customer level, basis the period of time and various alerts accumulated over other qualitative parameters the bank may consider adequate.		
c	The EWS must also provide multiple options for suitable statistical rating/scoring models to determine overall risk score to each loan account and overall, at a customer level.		
8	**Reporting Module:**		

a	Reports should be available as per specifications where the data has to be sent to RBI/ statutory boards.		
b	It should be possible to configure or generate various reports for real time/ near real time/ daily/ week/ Month/ Quarter/ Year as per the requirement of the Bank.		
c	Functionality of configurable dynamic dashboard and age-wise report the alerts for tracking the alert position.		
d	Reporting and Dashboards: Reports and dashboards tailored for different organizational levels (Branches, Specialized Branches, Regional Offices, Zonal Offices, and Central Office) based on relevance to each level.		
e	System shall provide a 360-degree dashboard of the customer, providing details including exposure, accounts, delinquencies, alerts generated, etc.		
9	**User Management Module:**		
a	The proposed solution should: Have capability to integrate with Active Directory for authentication check. Have option to add homogeneous set of users under one group. Allow to view/ update/ delete/ create groups. Have feasibility to provide privilege rights at each group level. Allow different type of users like Maker, Approver, Viewer & Admin to access the application. Have capability to add users automatically/ manually. Allow to create/ edit/ delete/ view users. Have capability to allocate user to specific groups. Provide information of user mapped to a role/group and vice versa.		
b	System should disallow multiple logins by a single user		
c	System shall have the capability to handle at least **1500** concurrent users at a time		
d	System shall have the capability to lock the screen if left attended for parameterized time, with options to logout or reactivate using Password		
10	**Artificial Intelligence and Machine Learning**		
a	The solution should filter and clean data to avoid false positives or negatives.		
b	The solution should validate historical data and present data for predictive analysis and probability of fraud.		
c	EWS solution should have advanced technologies like machine learning, artificial intelligence, and big data analytics to enhance the accuracy and efficiency of the solutions. The EWS package should be capable of giving scoring for an account based on the history of EWS alerts generated in the account and the same will be useful in the decision making of classifying an account as Red Flagged or otherwise.		
d	The proposed solution should provide in-built features and advanced techniques for the analyst to detect rare events, anomalies and outliers and/or influence points to help determine, capture or remove them from downstream analysis such as predictive models.		

Tender Processing Section

11	Technical Overview		
a	**Rack, Server, Network, Storage Software Specifications:** The proposed Solution should Provide Hardware, Associated Software and Racks as per specifications defined in **Annexure - 20.**		
b	**Disaster Recovery Center (DRC) Setup:** The proposed Solution's Hardware & Software at DC & DR shall be of same Configuration and Sizing, i.e. EWS Solution at DRC shall be exact replica of DC. **Except UAT Setup which will be available only at DC.**		
c	**DC-DR Configuration:** The EWS Solution at DC shall be in Production and DRC shall be in Standby mode. The roles will be reversed in case of Switchover if the situation arises.		
d	**Database Replication:** The Database Software shall provide an Automated Database Replication Solution to replicate data from DC to DR and vice versa to maintain Bank's defined **Recovery Point Objective (RPO) of 15 Minutes.**		
e	**DR Switchover:** The Solution should be able to Switch Over from DC to DR and Switch Back from DR to DC in case of any kind of Disaster or Planned Drill Activity maintaining the Bank's defined **Recovery Time Objective (RTO) of 120 Minutes** for the whole solution, with minimum notice time.		
f	**High Availability:** All the components of EWS Solution at each Site (DC & DR) Servers, Network devices, Software, database etc. shall be in **High Availability (HA) Configuration** allowing continuous operation within the Site, even if one component fails, by **automatic switching over** to a secondary system to minimize downtime and ensure service availability. Servers, Network Switches, SAN Switches must have redundant hardware to support the High Availability Configuration.		
g	**Cloud Migration:** The proposed solution should be deployed on Bank's premises. However, the solution should be **capable of seamless migration to cloud on demand.** The solution components should have an on-premise and on-cloud version. The proposed solution should support hybrid architecture which enables flexibility to host the platform either on-premise or on public/ private/ hybrid cloud at any point of time as required by the Bank to leverage advanced infrastructure technologies like containerization, micro services, server less computing and data mesh capabilities. Bidder should provide option to switch over to cloud at any point of time within the existing Subscription cost quoted with all the latest features. Bank can use cloud environment with the existing Subscription whenever required.		
h	**Backup Solution:** Bidder should provide onsite **Disk-To-Disk (D2D) backup** solution for taking backups of solution database and application on regular basis based on bank's backup policy at both DC and DR locations.		

	The Backup Solution should provide offsite **Disk-To-Tape (D2T) backup** for taking backup to tape to be kept at offsite location as per the bank's backup policy. The backup solution should include all necessary Hardware like backup storage and tape library and software to achieve the aforesaid purposes. The backup solution should be automated and monitored by the bidder's resident engineer. Onsite and Offsite Backups shall be restored periodically for Testing restorability of backups as per Bank's policy (Currently Quarterly). Bidder is to ensure availability of required Infrastructure for Testing Restoration.		
i	**Ticketing Tool/Portal:** The bidder must provide a Ticketing tool or portal to raise complaints/ issues in the proposed solution and to track the progress in resolving issues till its closure. Ticketing tool/portal should also provide the Turn Around Time (TAT) for problem-resolution. It should be able to provide the resolution status by portal Dashboard, emails and SMS as and when updated. The Ticketing tool is in addition to other means of raising complaints like emails.		
12	Market Intelligence Unit		
a.	Comprehensive monitoring of high-value corporate exposures through analytical insights derived from a variety of internal and external data sources		
b.	Creation and maintenance of a secure database of high-risk borrowers, enabling ongoing risk assessment and monitoring		
c.	Workflows that enable differentiated actions managed by a dedicated team, with role-based access controls to ensure appropriate data security and access segregation		
d.	Generation of network diagrams that identify linkages between corporates, directors, and related parties to help visualize complex relationships and connections		
e.	Highlighting the interconnectedness of entities by analyzing related party transactions		
f.	Detailed analysis of transaction history to identify patterns, anomalies, and potential risk indicators, supporting proactive risk management		

CANARA BANK Tender Processing Section

b. Non-Mandatory (Preferred) Requirements

The bidder should provide their response to the Non-Mandatory/ Preferred Technical and Functional Requirements by giving the compliance level as explained below. Explanations/suggestions of the bidder against each requirement should be given in the Remarks column. If more explanation of a point is needed, documents can be attached to Remarks Column of the respective requirement.

Compliance	Description	Marks
A	Already Available FULLY in the product.	1
B	Not Available but can be provided. Should be included in the version of the product being supplied before implementation. (Free of charge)	0.5
C	Not Feasible in the product due to architecture or structural limitations.	0

Sl No	Technical and Functional Requirements	Compliance A, B, C	Remarks
	Functional Requirements		
1	Automated data extraction from different source systems, without any manual intervention		
2	Data Integration Capabilities: Third Party Data Sources and internal data entry screen: The EWS system should have flexible integrating capabilities with third party data base (like rating agencies', credit bureaus, providers of ROC information) through formats such as APIs, JSON, XML, flat file upload etc.		
3	The EWS solution should be rich in the set of in-built transformations and functions that should include predefined table and column-level transformations including slowly changing dimensions.		
4	The tool should provide pre-build functionalities for the following: Financial Transformations Mathematical Transformations Statistical Computations		
5	EWS should have user interfaces for data profiling, data standardization, and clustering and data augmentation capabilities. In data profiling it should be able to conduct the following analysis: Structure discoveries Frequency distribution Pattern distribution Various statistical analysis Redundant data analysis		
6	Should support data cleansing and de-duplication, duplicate suspect processing, house holding, with array of out-of-the-box standardization rules conform data to corporate standards- or can build customized rules for special situations.		
7	Should have business rules and GUI' s for automatic merging and manual merging.		
8	The EWS solution should provide for master data management with semantic data description of input and output data sources uniquely identify each instance of a		

Sl No	Technical and Functional Requirements	Compliance A, B, C	Remarks
	business element customer, accounts, etc and standardize the master data to provide to provide a single source of truth.		
9	The proposed solution must have a utility capable of visualizing and extracting (text-mining) information relevant for the alerts from internal documents (such as stock audit reports, inspection reports, annual reports).		
10	The text mining utility should have algorithms to minimize false positives (Eg: Standard NLP libraries, stemming/lemmatization capabilities etc.)		
11	The text mining utility should be configurable for addition/deletion/modification of keywords/phrases and capable of identifying key words/phrases.		
12	The text mining utility should be capable of accepting bulk upload of documents.		
13	After processing document reference and the keyword searched to be included in the alert message.		
14	Text mining utility should have intelligent self-learning capability.		
	Transaction Monitoring		
Rule-Based Detection:			
15	The solution should allow authorized users to configure rule-level parameters such as frequency, display area (alert inbox/notifications), and TAT for alert closure.		
16	The EWSS should provide fuzzy logic as an option to carry out entity detection from unstructured data.		
17	The proposed solution should include a Predefined list of concepts to automatically identify common definitions Like company, person, date, location, time, etc. without a need to add new rules for them.		
18	Rules engine should have the ability to track changes to rules (i.e. who, when, what, why) (audit changes).		
19	Rules engine should have the functionality to retrieve historical activity and capture for rule creation/ maintenance.		
20	Ability to monitor transactions and events with pre-defined rules (as covered in rules library), generating alerts in near real-time.		
21	Authorized users to configure Scenario/ Rule manager functionality for the purpose of creation/ modification of alert scenarios and thresholds.		
22	Environment to perform regular testing and validation to assess the effectiveness of the monitoring system and incorporate any corrective measures to mitigate the same (Eg. False positive/ Erroneous Alerts detection and mitigation.)		
23	The proposed solution should be able to create networks based on both transaction as well as relationship based data, and create a nodes and links among the entities specified.		
24	The proposed solution should provide out-of-box entity analytics and direct intelligence analysts by showing		

CANARA BANK Tender Processing Section

Sl No	Technical and Functional Requirements	Compliance A, B, C	Remarks
	measures of centrality in entity networks - such as closeness, betweenness and influence to highlight suspicious borrowers/directors.		
25	The proposed solution should help analysts identify entity relationships that aren't obvious, traverse and query complex relationships, and uncover patterns and communities interactively.		
26	The proposed solution should provide in-built feature of Automated machine discovery to identify the core themes in the input document collection with associated relevance score.		
27	Rules engine should have the ability for allowing criteria to be defined/ modified (add, delete, create, update).		
28	Rules engine should be able to create a case based on externally and internally created scores as a decision element.		
29	The proposed solution should provide an in-built ability to create, modify and enable (or disable) custom concepts with validation checks within the same interactive interface.		
30	The proposed solution should include automated parsing (resume verification), tokenization and tagging.		
31	Capability to trigger notification mails/ SMS in an event of non-closure or delayed closure of an alert.		
32	EWSS should read unstructured data about accounts and use it for identifying early warning signals.		
33	EWSS should automatically assign sentiment to the text to identify the health of the account from an early risk perspective.		
34	EWSS should automatically identify organizations, person, locations mentioned in the article.		
35	EWSS should automatically discover rules for different early risk indicators like business risk, market risk, management risk, account risk, financial risk.		
36	Rules engine should have the ability to track changes to rules (i.e. who, when, what, why) (audit changes).		
37	Rules engine should be able to create/ modify exclusion criteria, within a rule, to route activity to an exclusion queue		
38	Rules engine should be able to create/ modify reactivation criteria, within the rule, for accounts that have previously been reviewed and excluded		
39	Solution should be able to define systemic actions at the rule level.		
40	Rules engine should be able to assign a unique case number to each item scored and actioned by the rules engine or out sorted for analyst review.		
41	EWSS should have ability to suppress unwanted alerts for an entity for a particular scenario.		
	Workflow Management		
42	Structured investigation workflows with predefined steps and trackable statuses.		
43	The proposed solution should allow the authorized users to create workflow path at every business rule level and		

Tender Processing Section

Sl No	Technical and Functional Requirements	Compliance A, B, C	Remarks
	configure workflows based on different alert categories and criticality.		
44	Functionality of automatic route and assign alerts to respective investigators based on pre-defined case routing logic without any delay after generation of alert.		
45	The workflow module should support dynamic routing configurations to facilitate both centralized and decentralized case management and provide flexibility to adjust routing dynamically based on predefined criteria such as risk level, case type, loan portfolio, or other risk indicators, ensuring that cases are handled by the appropriate team regardless of their origination point.		
46	Enable time-based triggers and reminders for each workflow step to ensure timely action on cases.		
47	Configurable notifications (email, SMS, in-app,) for alert assignment, case updates, escalations, pending actions, and other key events and reminders to assigned users for pending tasks related to each case to ensure timely follow-up.		
48	Flexibility to adjust routing dynamically based on predefined criteria such as risk level, case type, loan portfolio, or other risk indicators, ensuring that cases are handled by the appropriate team regardless of their origination point.		
49	EWS should have advanced routing rules to route along any data event.		
50	The user should have ability to apply a mass action to case-close, append etc.		
51	The user should have ability to link cases under investigation.		
52	In case of alerts where standardized actions have to be taken EWS must have automated case processing framework.		
53	EWS have ability to add several alerts to one case.		
54	EWS should have the ability to rate cases by priority, high to low to the analyst role in the queue. New Cases will populate the queue according to the priority.		
55	Enable data export options (e.g., CSV, PDF) for further analysis or regulatory reporting.		
56	EWS should provide the ability to perform systematic actions based upon an analyst's work action.		
57	Screen flow and system process must represent the task workflow.		
58	EWS should be able to define the systematic actions to be taken, based upon an analyst's work action.		
59	Power users should have the ability to configure standard workflows to route case activities to. appropriate teams.		
60	Alerts should be managed by more than one appointed person using workflow functionality.		
61	Reports review and appropriate reaction could be managed by more than one appointed person using workflow functionality.		
62	Workflow actions should not be deleted or altered after submission.		

CANARA BANK Tender Processing Section

Sl No	Technical and Functional Requirements	Compliance A, B, C	Remarks
63	Internal employee should not be able to delete/modify/recreate workflow steps without appropriate access rights (access rights to administrations only).		
64	EWS should provide different access rights for different users.		
65	System should: Suggest followup actions for every alert based on policies set by the Risk/Monitoring teams. Enable extended workflow capabilities beyond alert closure, for committee decisioning such as RFA tagging, fraud reporting, etc. Support a TAT for alert closure which can vary by alert. Support multi-level workflows based on conditions such as Department, etc Facilitate bulk closure of alerts based on common conditions. Provide access to workflow functionalities such as alert closure and approval over mobile, for anywhere, anytime access. Support workflow overrides such as exceptions for large branches, etc. Allow authorised users to tag an account as an RFA for tracking purposes. Support two-way workflows, i.e., Alerts submitted by L1 officer could be rejected by L2 officer for corrections and resubmission, with suitable remarks and supporting documents. Enable users to tag alerts as false positives in order to prevent them from flowing throughout the hierarchy. Support configurable workflows and dynamic routing based on predefined business rules such as based on exposure, criticality, etc. Support rule management within the workflow engine that allows for flexible configuration and conditional logic based on case properties. **System should have the reverse feedback capabilities.**		
	Alert Generation and Scoring:		
66	EWS should have capability to group alerts into single entity actionable events.		
67	framework that assigns provides an overall risk score to each loan account and overall at a customer level, basis the various alerts accumulated over a period of time and other qualitative parameters the bank may consider adequate.		
68	Separate module accessible by Branches and Other offices for reporting Behavioural (Non-Transaction Based) alert scenarios.		
69	The proposed EWS solution should have capability to utilize past alerts for a certain period to assign criticality of alert.		

Sl No	Technical and Functional Requirements	Compliance A, B, C	Remarks
70	The EWS is expected to have features for scoring alerts based on suitable formulae.		
71	EWS should have ability to suppress unwanted alerts on the following parameters: permanently or duration based for a Particular geography of operations for a particular industry for a particular entity/group of entities or a combination of the above.		
72	The EWS is expected to have features for setting a time validity for certain alerts.		
73	EWS should be able to differentiate between cases which were created from alerts versus those which were created manually		
74	The proposed application should be capable of maintaining history of alerts generated and provide a framework for trend analysis.		
	Web Harvesting		
75	The system should have web harvesting capabilities to search for news items (including regional languages), articles etc. relevant for the purpose of alert generation.		
76	The web harvesting application should be capable of integrating to feeds from various business/news/security exchange/social websites (based on a schedule).		
	Reporting and Audit Trail:		
77	The system should be capable in providing drill down reports with Account wise, Branch wise. Customer wise, Industry wise, Sector wise, Zonal wise, Size wise, etc.		
78	Availability of customized dashboard as per user requirement without intervention of the vendor.		
79	Customizable Reports/ Dashboards for Decision making/ Audit/ Internal reporting purposes.		
80	The system should be able to provide configurable reports like Amount in Full, Lakhs, Millions etc.		
81	The system should be capable In providing drill down reports with Account wise, Branch wise, Customer wise, Industry wise, Sector wise, Zonal wise, Size wise, etc,		
82	The system should be capable of risk categorization of borrowers based on frequency/ gravity of Alerts		
83	The solution should support distribution of Reports and Dashboards to iOS and Android devices. The Native App should be freely available for iOS on App Store and for Android devices on Google play-		
84	Reports and Dashboards access on iOS and Android devices should be using native application which helps leverage most popular gestures and capabilities, including zoom, swipe, etc. to optimize ease of use and user engagement.		
85	The solution should support same dashboard / report created on Web to be accessed from iOS and Android devices without requiring any redesign.		

Tender Processing Section

Sl No	Technical and Functional Requirements	Compliance A, B, C	Remarks
86	The solution should provide collaboration support with Annotation on Mobile devices.		
	Artificial Intelligence and Machine Learning capabilities		
87	Identification of transactional patterns and typologies, incl. Link analysis.		
88	Train models using Bank's existing historical transaction & alert data labelled as either suspicious or legitimate.		
89	Risk scoring of EWS alerts based on history of alert resolutions and reporting, along with other parameters eg. Customer demographics, Account activity/ vintage, History of Alert generation/RFA/Fraud, etc.		
90	Predictive models to identify complex and evolving patterns of suspicious behaviour.		
91	Estimation of optimum thresholds for alert scenarios based on history of True/ False positives and True/ False negatives.		
92	Comprehensive monitoring of high-value corporate exposures through analytical insights derived from a variety of internal and external data sources.		
93	Optical Character Recognition (OCR) for capturing information from PDFs/Images (such as stock audit reports, inspection reports, annual reports, meeting agendas and meeting minutes)		
94	The proposed solution should identify linkages among seemingly unrelated transactions and uncover unknown relationships through a network visualization interface		
95	Grouping Alerts, Customers and Accounts with similar characteristics and transactional behaviours together		
	User Interface		
96	User friendly and Customizable Interface with access rights and modules differentiated based on User, Office, etc.		
97	Integration to Bank's Single Authentication System (SAS) for enabling User creation/ deletion and Biometric login to the solution.		
98	The proposed solution should provide features for visualization, navigating and drilling into listed transactions, scenarios that triggered the alerts		
99	Charts, Graphs and other Visual representations of information (e.g., Alert pendency, RFA, Fraud, Probability of RFA, etc.,)		
100	The proposed solution should support local languages and culturally relevant formats.		
	Maximum Marks - 100		

Notes:

a. Total marks will be the sum of maximum marks (1 marks) of the non-mandatory/ preferred Technical and Functional requirements mentioned above.

b. The bidder should score minimum 70% marks from the above non-mandatory/ preferred Technical & Functional requirements against total marks to qualify under the Technical Proposal evaluation.

c. Any specification declared Compliant, however, it is found non-compliant during Technical evaluations based on the demonstration or POC (if called for) will lead to disqualification.

d. Bidder should showcase above specifications/ features and provide equivalent document.

e. **Bidder to note that all features marked as "a" (Already Available FULLY in the product), and agreed by the bidder, must be available for demonstration during "Presentation and Product Demonstration".** During evaluation, if any of the criteria mentioned as compliant is not found in the solution, marking will be modified in the respective category as evaluated by the Bank & Bank's decision shall be binding on the bidders.

Declaration:

1. We hereby confirm that we have various certificates/bench mark testing standards for the items quoted to meet the intent of the Bid.
2. We hereby confirm that we have back to back arrangements with third party software/ cloud for providing continuous and un-interrupted support to meet SLAs obligations as per bid terms.
3. We hereby confirm that the information submitted above is true to the best of our knowledge. We understand that in case any discrepancy is found in the information submitted by us our tender is liable to be rejected.

Date:
Place:

Signature with seal
Name:
Designation:

SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS

1. **Amended Project Timelines**

1.1. Bank shall provide the address and contact details for delivery of required hardware/software items for implementation of Solution while placing the order.

1.2. The vendor shall submit the acceptance of the Purchase Order within seven (7) days from the date of issue of Purchase Order. In case of non-receipt of acceptance by the due date, the Purchase Order shall deem to have been accepted by the vendor.

1.3. **The Further timeline shall be as follows:**

Sl. No.	Particulars	Timeline
1.3.1	Delivery of Hardware & other Items (including OS) at DC, DRC & UAT Locations	Within **eight (08) weeks** from the date of acceptance of Purchase Order or **nine (09) weeks** from the date of issue of Purchase Order.
1.3.2	Installation, Integration and Commissioning of Hardware & Other Items (including OS) at DC, DRC & UAT Locations	The selected bidder should ensure installation, configuration, Integration and commissioning of the delivered Hardware and other items at the bank branch/office within **Four (4) weeks** from the date of delivery of all the materials for each ordered location.
1.3.3	Installation, Integration, and Implementation of EWS Software.	The selected bidder should ensure Installation, Integration and implementation of EWS Software at the bank specified location within four (04) weeks from the date of Installation, Integration and Commission of Hardware & Other Items (including OS)
1.3.4	User Acceptance Testing, Data Migration, Training and Pilot Run of the EWS Solution	The selected bidder should complete User Acceptance Testing, Data Migration, Training and Pilot Run of the EWS Solution at the Bank specified location within four (04) weeks from the date of Installation, Integration and Implementation of EWS Software.
1.3.5	Full EWS Solution Implementation, Documentation and Go-Live of the proposed EWS solution with AI/ML implementation at DC, DRC.	The selected bidder should ensure delivery of the Enterprise Licenses for EWS Solution, installation, integration, implementation and go-live of the proposed EWS solution with AI/ML implementation within four (04) weeks from the date of Successful UAT testing and Pilot Run.

1.4. The installation will be deemed as incomplete if the hardware/ software/ OS/ database/ any other required software is not delivered or is supplied but not installed and/or not operational or not acceptable to Canara Bank after acceptance testing/ examination.

1.5. The solution will be accepted after complete integration and satisfactory working of the solution.

1.6. Bank reserves the right to change/modify locations for supply of the items. In the event of any change/modification in the locations where the hardware items are to be delivered, the bidder in such cases shall deliver, install and commission at the modified locations at no extra cost to the Bank during the contract period. However, if the hardware items are already delivered, and if the modifications in locations are made after delivery, the bidder shall carry out installation and commissioning at the modified locations and the Bank in such cases shall bear the shifting charges/arrange shifting as mutually agreed. The Warranty/ATS/AMC and all RFP terms should be applicable to the altered locations also.

1.7. The Installation will be deemed as incomplete if any component of the Solution is not delivered or is delivered but not installed and/ or not operational or not acceptable to the Bank after acceptance testing/ examination. In such an event, the supply and installation will be termed as incomplete, and system(s) will not be accepted. The installation will be accepted only after complete commissioning of Solution.

1.8. The Bank will not arrange for any Road Permit/ Sales Tax clearance for delivery of hardware to different locations and the selected bidder is required to make the arrangements for delivery of hardware to the locations as per the list of locations/ items provided from time to time by the Bank. However, the Bank will provide letters/ certificate/ authority to the selected bidder, if required.

1.9. Partial or incomplete or damaged delivery of materials will not be considered as delivered of all the ordered materials. Date of delivery shall be treated as date of last material delivered to the ordered locations if materials are not damaged. In case materials are delivered with damage, Date of delivery shall be treated as date of replacement of damaged material with new one. Delivery payment shall be paid against completion of delivery of all the ordered materials without any damage and proof of delivery duly certified by Bank's Officials, along with delivery payment claim letter.

1.10. End to End implementation of the solution will be deemed as complete only when the same is accepted by the Bank and sign off given in accordance with the terms & conditions of this RFP and satisfactory working of the solution.

Annexure-10

Technical Evaluation Criteria

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

SUB: Selection of vendor for end to end implementation and maintenance of comprehensive centralized Early Warning Signal (EWS) Solution for a period of five years in Canara Bank.

Ref: GEM/2025/B/5787764 dated 06/01/2025.

The technical evaluation of the bidder will be carried as per the details furnished below:

Sl. No.	Evaluation Parameters	Documents to be submitted	Max marks
1.	**Capability of the Bidder.** The bidder should have implemented and maintaining any Banking related IT solution in atleast One (01) of the Scheduled Commercial Banks, with minimum 2000 branches in India as on RFP date. Implementation Experience • 3 or more implementations - 10 Marks • 2 implementations - 7 Marks • 1 implementation - 5 Marks	The bidder should submit Purchase Order/Work order/contract agreement along with satisfactory performance letter/reference letter from the customer duly mentioning the details of the solution including name of the OEM and sign-off.	10
2.	Successful Implementation of EWS Solution proposed by the bidder. **The proposed EWS Solution should have been successfully implemented and maintained within the last 3 years in atleast one (01) of the Scheduled Commercial Banks having more than 2000 branches in India as on RFP date.** Each implemented EWS Solution in the bank must have at least "Rule/Scenario (RBI/DFS/BANK) based Alert Generation" as part of its scope. Implementation of proposed EWS Solution, • More than and equal to 5000 Branches in India - 20 Marks • • More than and equal to 3500 branches but less than 5000 Branches in India - 15 Marks • More than 2000 but less than 3500 Branches in India - 10 Marks	**The Bidder has to submit Purchase Order/Work order/contract agreement along with along with satisfactory project completion certificate/ Reference letter from the Client to confirm this from bidder/OEM,** having "Rule/Scenario based Alert Generation" as part of its scope and project sign off.	20
3.	Compliance to Functional and Technical Requirements as per point b Non-Mandatory [Preferred] Requirements) of Annexure-9.	As per Technical & Functional Compliance based on the responses from the Bidder as per the Point b. (Non-Mandatory	40

		[Preferred] Requirements) of Annexure-9 and to be demonstrated at "Presentation & Product Demonstration" and assessed by Bank. The total marks scored by the bidder in Point b. (Non-Mandatory [Preferred] Requirements) of Annexure-9 shall be normalised to the maximum marks subjected against this parameter. Bidder to note that all features, agreed by the bidder, must be available for demonstration during "Presentation and Product Demonstration". During evaluation, if any of the criteria mentioned as compliant is not found in the solution, marking will be modified in the respective category as evaluated by the Bank & Bank's decision shall be binding on the bidders.	
4.	Presentation by the Bidder: ** Note: The Presentation is as per the technical & functional requirement/scope of work/other terms as mentioned in RFP to the Bank.	Points will be assigned by an internal committee based on the methodology, work plan, team composition and presentations. As per Table P-1	30
	Total Marks		100

****Bidder should provide Onsite visit to verify the existing EWS package if required.**

Note: The bidder should score minimum 70% marks (i.e., 70 Marks out of 100 marks) total marks for qualifying under Technical Evaluation. The bidders qualified under Technical Proposal Evaluation will be eligible for commercial opening.

Presentation of proposal:

Canara Bank will schedule the presentations and intimate the time and locations to the bidders. Failure of a bidder to complete a scheduled presentation may result in the rejection of that Bidder's proposal.

Table P-1

Sl. No.	Presentation Agenda	Details	Max Marks
1.	Proposed Solution Demo in UAT of the bidder.	Demo of the proposed Solution to be presented with multiple scenarios.	10
2.	Project Implementation plan	Detailed Plan to implement the project scope.	5
3.	IT architecture, Approach, Security Aspects and Methodology.	The IT architecture and security features of the proposed solution. Flexibility of the solution for GUI.	5
4.	Project Governance and Project Team	Details of qualified & experienced resources provided in the respective modules.	5

5.	Post Implementation Support	Compliance with the regulatory guidelines and coordination with the bank as well timely resolution of problems.	5
Maximum Marks for Presentation			30

Bidders achieving the minimum passing mark 70% will be considered eligible for Commercial evaluation process.

The Bank may, at its sole discretion, decide to seek more information from the bidders in order to normalize the bids. However, bidders will be notified separately, if such normalization exercise is resorted to.

Terms & Conditions

a. Bank reserves the right to conduct interviews of the proposed team members.

b. In case of absence of the allotted resource, the standby should perform the job of the absentee.

c. Bank may reject such manpower if bank is not satisfied with his/her performance.

Declaration: We hereby confirm that the information submitted above is true to the best of our knowledge. We understand that in case any discrepancy is found in the information submitted by us, our response to this RFP is liable for rejection.

Date:
Place:

Signature with seal
Name:
Designation:

Amended Appendix-G
Draft Contract Agreement

CONTRACT AGREEMENT FOR ..... AS PER THE PURCHASE ORDER ..... DATED .....

THIS AGREEMENT (the Agreement) executed at Bengaluru on ..... day of ..... 202.....

BETWEEN

Canara Bank, a body corporate constituted under the Banking Companies (Acquisition and Transfer of Undertakings) Act 1970, having its Head Office at 112, J C Road, Bengaluru - 560002 in India, represented by the Authorised Signatory of its CP & VM Wing, Mr. ....., (Designation) , (hereinafter referred to as "PURCHASER") which expression shall unless excluded by or repugnant to the subject or context be deemed to mean and include its assigns and successors) of the **ONE PART**

AND

M/s ....., a Company/Firm constituted and registered under the provisions of the Companies Act 1956 having its Registered Office at ..... represented by the Authorized Signatory, Mr..... (Designation) (hereinafter referred to as "Vendor /service provider" which expression shall unless excluded by or repugnant to the subject or context be deemed to mean and include its administrators, successors and assigns) of the **OTHER PART**:

The Purchaser and Vendor/service provider are hereinafter collectively referred to as "Parties".

WHEREAS the Purchaser invited Bids for Products/Services VIZ ....., (Brief description of product/service/solutions) and has accepted the Bid by the Vendor/service provider for ..... (Full description of product/service/solutions) for the sum of Rs..... (Rupees ..... only) exclusive of GST (herein after called "the Contract Price").

NOW THIS AGREEMENT WITNESSETH AND IT IS HEREBY AGREED BY AND BETWEEN THE PARTIES HERETO AS FOLLOWS:

1. **DEFINITION AND INTERPRETATION:**

1.1 In this Agreement words and expressions shall have the same meanings as are respectively assigned to them in the terms and conditions of RFP/RFQ/EOI/ Amendments/ LOI/ Purchase Order referred to.

1.2 Reference to a "Business day" shall be construed as reference to a day (other than a Sunday, second or fourth Saturday) on which banks in the State are generally open for business;

1.3 any reference to a month shall mean a reference to a calendar month as per the Gregorian calendar;

1.4 In this Agreement, unless the context otherwise requires:

1.4.1 words of any gender are deemed to include the other gender;

1.4.2 words using the singular or plural number also include the plural or singular number, respectively;

1.4.3 the terms "hereof", "herein", "hereby", "hereto" and any derivative or similar words refer to this entire Agreement;

1.4.4 headings, sub-headings and bold typeface are only for convenience and shall be ignored for the purposes of interpretation;

1.4.5 reference to any legislation or law or to any provision thereof shall include references to any such legislation or law as it may, after the date hereof, from time to time, be amended, supplemented or re-enacted, and any reference to a statutory provision shall include any subordinate legislation made from time to time under that provision;

1.4.6 any term or expression used, but not defined herein, shall have the same meaning assigned thereto under the RFP;

1.4.7 references to the word "include" or "including" shall be construed without limitation;

1.5 The RFP/RFQ/EOI Document/ Bid No/PO No ..... dated ..... as amended from time to time and this Agreement, and the other related documents shall be deemed to form and be read and construed as part of this Agreement, which, inter alia, includes

a) The Bid Form and the Price Schedule submitted by the Bidder.
b) The Bill of Material.
c) The Technical & Functional Specifications.
d) The Terms and Conditions of the Contract.
e) The Purchaser's Letter of Intent/Notification of Award.
f) Schedule of Dates, Amounts etc.
g) Pre-Contract Integrity Pact.
h) All pre bid clarifications/mail communications shared with the bidder during the processing of this bid.

All the above are collectively referred to as "the Transaction Documents" forming an integral part of the Contract are to be taken as mutually explanatory to one another. Detailed site orders as and when released shall form an integral part of this contract. However, in case of conflict between the Clauses of the Contract and Schedules appended to the Contract, provisions of the Clauses of the Contract shall prevail.

2. SCOPE OF WORK:

The scope of work shall be as Per RFP/RFQ/EOI Document/ Bid No/PO No ..... Dated.....

3. TERM OF THE CONTRACT:

The contract shall be valid for the full duration till completion of all contractual obligations by the Vendor/Service Provider and PURCHASER for the current orders or further orders to be released to Vendor/ Service Provider as per the terms and conditions in this contract or till the expiry of the contract whichever is later.

4. PAYMENT TERMS:

The payment terms shall be as specified in the RFP/RFQ/EOI Document/ Bid No/PO No ..... dated .....

5. PENALTIES/LIQUIDATED DAMAGES:

As Per RFP/RFQ/EOI Document/ Bid No/PO No ..... dated .....

6. SECURITY DEPOSIT / PERFORMANCE BANK GUARANTEE:

The Vendor/Service Provider shall submit Security Deposit/Performance Bank Guarantee as specified in the RFP/RFQ/EOI Document/ Bid No/PO No ..... dated .....

7. ASSIGNMENT:

7.1. VENDOR/ SERVICE PROVIDER shall not assign to any one, in whole or in part, it's obligations to perform under the Contract, except with the BANK's prior written consent.

7.2. If the BANK undergoes a merger, amalgamation, take-over, consolidation, reconstruction, change of ownership etc., this Contract shall be considered to be assigned to the new entity and such an act shall not affect the rights and obligations of the VENDOR/ SERVICE PROVIDER under this Contract.

8. SUB-CONTRACTING:

8.1. VENDOR/ SERVICE PROVIDER shall not subcontract or permit anyone other than its personnel to perform any of the work, service or other performance required of the VENDOR/ SERVICE PROVIDER under the contract without the prior written consent of the BANK.

8.2. Notwithstanding the above or any written consent granted by the Bank for subcontracting the services, the Vendor/Service Provider alone shall be responsible for performance of the services under the contract.

9. SERVICE LEVELS:

9.1. During the term of the contract, the vendor shall maintain the Service Levels as detailed in RFP/GeM Bid/PO. In case the vendor fails to maintain the Service Levels, Liquidated damages as detailed in RFP/GeM Bid/PO shall be imposed on the Vendor/Service provider.

9.2. In relation to any undertaking and under any circumstances, the service provider shall exercise the degree of skill, diligence, prudence, and foresight that would reasonably be expected from a highly skilled and experienced professional engaged in the same type of undertaking under similar circumstances. Further the vendor/service provider shall identify and designate skilled personnel necessary for the operation of critical functions under this agreement. Such personnel shall be considered essential and must be available to work on-site during exigencies including but not limited to emergencies and pandemics. The service provider shall provide the bank with a list of these essential personnel and any associated backup arrangements and ensure their availability as required.

9.3. The service provider shall wherever applicable be obligated to establish and maintain suitable back-to-back contractual arrangements with the Original Equipment Manufacturers (OEMs) to ensure that all services, warranties, and obligations stipulated in this Agreement are fully supported and enforceable by the OEMs. These arrangements shall include, but are not limited to, the OEMs' commitment to provide necessary resources, technical support, replacement parts, and any other services required to fulfill the terms of this Agreement. The Service Provider must provide evidence of such arrangements upon request and

shall ensure that these agreements are in place for the duration of this contract to guarantee seamless service delivery and compliance with all contractual obligations.

9.4. The vendor/service provider shall deliver the agreed-upon goods and services in accordance with this agreement with respect to quality and quantity, and shall be subject to regular monitoring and reporting.

10. ORDER CANCELLATION/TERMINATION OF CONTRACT:

10.1. The Bank reserves its right to terminate this CONTRACT at any time without assigning any reasons, by giving a 30 day's notice.

10.2. The Bank reserves its right to cancel the entire / unexecuted part of CONTRACT at any time by assigning appropriate reasons and recover expenditure incurred by the Bank in addition to recovery of liquidated damages in terms of the contract, in the event of one or more of the following conditions:

10.2.1. Delay in delivery beyond the specified period for delivery.

10.2.2. Serious discrepancies noted in the items delivered.

10.2.3. Breaches in the terms and conditions of the Order.

10.2.4. Non submission of acceptance of order within 7 days of order.

10.2.5. Excessive delay in execution of order placed by the Bank.

10.2.6. The Vendor/Service Provider commits a breach of any of the terms and conditions of the bid.

10.2.7. The Vendor/Service Provider goes in to liquidation voluntarily or otherwise.

10.2.8. An attachment is levied or continues to be levied for a period of 7 days upon the effects of the bid.

10.2.9. The progress made by the Vendor/Service Provider is found to be unsatisfactory.

10.2.10. If deductions on account of liquidated Damages exceeds more than 10% of the total contract price.

10.3. Bank shall serve the notice of termination to the Vendor/Service Provider at least 30 days prior, of its intention to terminate services.

10.4. In case the Vendor/Service Provider fails to deliver the quantity as stipulated in the delivery schedule, the Bank reserves the right to procure the same or similar materials from alternate sources at the risk, cost and responsibility of the Vendor/Service Provider by giving 7 days' prior notice to the Vendor/Service Provider.

10.5. After the award of the contract, if the Vendor/Service Provider does not perform satisfactorily or delays execution of the contract, the Bank reserves the right to get the balance contract executed by another party of its choice by giving one months' notice for the same. In this event, the Vendor/Service Provider is bound to make good the additional expenditure, which the Bank may have to incur for the execution of the balance of the order/contract. Such additional expenditure shall be incurred by the bank within reasonable limits & at comparable price prevailing in the market. This clause is also applicable, if for any reason, the contract is cancelled.

10.6. The Bank reserves the right to recover any dues payable by the Vendor/Service Provider from any amount outstanding to the credit of the Vendor/Service

Provider, including the pending bills and security deposit, if any, under this contract.

10.7. In addition to the cancellation of purchase order, the Bank reserves its right to invoke the Bank Guarantee or foreclose the Security Deposit given by the Vendor/Service Provider towards non- performance/non-compliance of the terms and conditions of the contract, to appropriate towards damages.

10.8. Notwithstanding the existence of a dispute, and/ or the commencement of negotiation and mediation proceedings, Vendor/Service Provider should continue the services. Vendor/Service Provider is solely responsible to prepare a detailed Reverse Transition plan.

10.9. The Bank shall have the sole decision to determine whether such plan has been complied with or not. Reverse Transition mechanism would include services and tasks that are required to be performed/ rendered by the Vendor/Service Provider to the Bank or its designee to ensure smooth handover and transitioning of the Bank's deliverables.

11. EXIT MANAGEMENT PLAN:

11.1. Vendor/Service Provider shall submit a structured & detailed Exit Management plan along with Training and Knowledge transfer for its exit initiated by the Bank.

11.2. Vendor/Service Provider shall update the Transition and Exit management on half yearly basis or earlier in case of major changes during the entire contract duration. The plan and the format shall be discussed and approved by the Bank.

11.3. The exit Management plan shall deal with the following aspects but not limited to of exit management in relation to the Service Level as a whole and in relation to in scope applications, interfaces, infrastructure and network and the scope of work.

11.3.1 A detailed program of the transfer process that could be used in conjunction with a replacement vendor including details of the means to be used to ensure continuing provision of the services throughout the transfer process or until the cessation of the services and of the management structure to be used during the transfer.

11.3.2 Plans for provision of contingent support to the Project and replacement Vendor/Service Provider for a reasonable period (minimum three month and maximum as per mutual agreement) after transfer or as decided by Canara Bank.

11.3.3 Plans for training of the Replacement Service Provider/Canara Bank staff to run the operations of the project. This training plan along with the training delivery schedule should be approved by Canara Bank. The delivery of training along with handholding support and getting the sign off on the same would be the responsibility of Vendor/Service provider.

11.4. At the end of the contract period or during the contract period, if any other Service Provider is identified or selected for providing services related to Vendor/Service Provider scope of work, they shall ensure that a proper and satisfactory handover is made to the replacement Service Provider. This transition process shall be managed to ensure minimal disruption to the bank's operations and continuity of services.

11.5. All risk during transition stage shall be properly documented by Vendor/Service Provider and mitigation measures shall be planned to ensure a smooth transition without any service disruption. Vendor/Service Provider must ensure that hardware supplied by them shall not reach end of support products (software

hardware) at time of transition. Vendor/Service Provider shall inform well in advance end of support products (software/hardware) for the in-scope applications and infrastructure.

11.6. The transition & exit management period will start minimum six (6) months before the expiration of the contract or as decided by Canara Bank.

11.7. Vendor/Service Provider will provide shadow support for a minimum of 90 days or as decided by the Bank before the end of termination of notice period or expiry of the contract as applicable at no additional cost to the Bank.

11.8. In case of termination, the exit management period will start from effective date of termination, or such other date as may be decided by Canara Bank and communicated to Vendor/Service Provider.

11.9. Vendor/Service Provider must ensure closing off all critical open issues, any audit observation as on date of exit. All other open issues as on date of Exit shall be listed and provided to Canara Bank.

11.10. Vendor/Service Provider needs to comply with Banks requirements and any statutory or regulatory guidelines during the reverse transition period.

11.11. The vendor/service provider shall fully cooperate with relevant authorities in the event of the bank's insolvency or resolution, including providing necessary information and support as required to facilitate the orderly transition and resolution process, ensuring minimal disruption to services and compliance with regulatory requirements.

12. TRAINING AND HANDHOLDING:

12.1. Vendor/Service Provider shall provide necessary knowledge transfer and transition support to the satisfaction of the Bank. The deliverables as indicated below but not limited to:

12.1.1. Entire back-up History but not limited to archive policies, retention policies, restore policies, schedules, target storage, backup history.

12.1.2. Change Request Logs

12.2. Assisting the new Service Provider/Bank with the complete audit of the system including licenses and physical assets

12.3. Detailed walk-throughs and demos for the solution

12.4. During the exit management period, the Vendor/Service Provider shall use its best efforts to deliver the services.

12.5. Vendor/Service Provider shall hold technical knowledge transfer sessions with designated technical team of Business and/or any replacement Service Provider in at least last three (3) months of the project duration or as decided by Bank.

During Reverse Transition Bank will not pay any additional cost to the Vendor/Service Provider for doing reverse transition.

13. INTELLECTUAL PROPERTY RIGHTS:

13.1. VENDOR/ SERVICE PROVIDER warrants that the inputs provided shall not infringe upon any third party intellectual property rights, including copyrights, patents and other intellectual property rights of any nature whatsoever. VENDOR/ SERVICE PROVIDER warrants that the deliverables shall not infringe upon any third party

intellectual property rights, including copyrights, patents and other intellectual property rights of any nature whatsoever. VENDOR/ SERVICE PROVIDER shall ensure that the Solution supplied to the BANK shall not infringe the third party intellectual property rights, if any. VENDOR/ SERVICE PROVIDER shall ensure that third party rights are not infringed even in case of equipment /software supplied on behalf of consortium as VENDOR/ SERVICE PROVIDER.

13.2. In the event that the Deliverables become the subject of claim of violation or infringement of a third party's intellectual property rights, VENDOR/ SERVICE PROVIDER shall at its choice and expense:

13.2.1. Procure for BANK the right to continue to use such deliverables.

13.2.2. Replace or modify such deliverables to make them non-infringing, provided that the same function is performed by the replacement or modified deliverables as the infringing deliverables or

13.2.3. If the rights to use cannot be procured or the deliverables cannot be replaced or modified, accept the return of the deliverables and reimburse BANK for any amounts paid to VENDOR/ SERVICE PROVIDER for such deliverables, along with the replacement costs incurred by BANK for procuring equivalent equipment in addition to the penalties levied by BANK. However, BANK shall not bear any kind of expense, charge, fees or any kind of costs in this regard. Notwithstanding the remedies contained herein, VENDOR/ SERVICE PROVIDER shall be responsible for payment of penalties in case service levels are not met because of inability of the BANK to use the proposed solution.

13.3. The indemnification obligation stated in this clause shall apply only in the event that the indemnified party provides the indemnifying party prompt written notice of such claims, grants the indemnifying party sole authority to defend, manage, negotiate or settle such claims and makes available all reasonable assistance in defending the claims [at the expenses of the indemnifying party]. Notwithstanding the foregoing, neither party is authorized to agree to any settlement or compromise or the like which would require that the indemnified party to make any payment or bear any other substantive obligation without the prior written consent of the indemnified party. The indemnification obligation stated in this clause reflects the entire liability of the parties for the matters addressed thereby.

13.4. VENDOR/ SERVICE PROVIDER acknowledges that business logics, work flows, delegation and decision making processes of BANK are of business sensitive nature and shall not be disclosed/referred to other clients, agents or distributors of Software/Service.

14. INDEMNITY:

14.1. VENDOR/ SERVICE PROVIDER shall keep and hold the Bank indemnified and harmless from time to time and at all times against all actions, proceedings, claims, suits, liabilities (including statutory liability), penalties, demands, charges, costs (including legal costs) and expenses, damages, losses and any other expenses which may be caused to or suffered by or made or taken against the Bank arising out of:

14.1.1. The breach, default or non-performance of undertakings, warranties, covenants or obligations by VENDOR/ SERVICE PROVIDER;

14.1.2. Any contravention or Non-compliance with any applicable laws, regulations, rules, statutory or legal requirements by VENDOR/ SERVICE PROVIDER;

14.1.3. Fines, penalties, or punitive damages levied on Bank resulting from supervisory actions due to breach, default or non-performance of undertakings, warranties, covenants, or obligations by the Vendor/Service Provider

14.2. Vendor/Service Provider shall be liable for any loss caused to the bank due to any wilful negligence /malpractice by the Vendor/Service Provider or any of its officers, employees, agents or representatives which is found to be a causative factor for any fraud in spite of liability under the relevant statute, civil and/ or criminal as the case may be, for any malicious acts, negligent acts, wrongful acts, fraudulent acts and/ or offline transactions committed (including those committed by any of its employees, agents and/or representatives) in the performance of the Services under this Agreement and shall not be deemed to be acting on or behalf of the Bank in any manner whatsoever to the extent of such acts and/ or transactions.

14.3. VENDOR/ SERVICE PROVIDER shall indemnify, protect and save the Bank against all claims, losses, costs, damages, expenses, action suits and other proceedings, resulting from infringement of any law pertaining to patent, trademarks, copyrights etc. or such other statutory infringements in respect of **Solution** supplied by them.

14.3.1. All indemnities shall survive notwithstanding expiry or termination of the contract and bidder shall continue to be liable under the indemnities.

14.3.2. The limits specified in below clause shall not apply to claims made by the Bank/third parties in case of infringement of Intellectual property rights or confidential information, fraud or gross negligence or wilful misconduct or for claims relating to the loss or damage to real property and tangible personal property and for bodily injury or death and in these cases the liability will be unlimited.

14.3.3. All Employees engaged by VENDOR/ SERVICE PROVIDER shall be in sole employment of VENDOR/ SERVICE PROVIDER and the VENDOR/ SERVICE PROVIDER shall be solely responsible for their salaries, wages, statutory payments etc. That under no circumstances shall the Bank 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 bidder.

14.4. VENDOR/ SERVICE PROVIDER's aggregate liability shall be subject to an overall limit of the total Cost of the project.

15. RIGHT TO AUDIT:

15.1. The VENDOR has to get itself annually audited by internal/ external empanelled Auditors appointed by the PURCHASER/inspecting official from the Reserve Bank of India or any regulatory authority, covering the risk parameters finalized by the PURCHASER/such auditors in the areas of products (IT hardware/software) and services etc., provided to the PURCHASER and the VENDOR is required to submit such certification by such Auditors to the PURCHASER. The VENDOR and or his/their outsourced agents/subcontractors (if allowed by the PURCHASER) shall facilitate the same. The PURCHASER can make its expert assessment on the efficiency and effectiveness of the security, control, risk management, governance system and process created by the VENDOR. The VENDOR shall, whenever required by the Auditors, furnish all relevant information, records/data to them. All costs for such audit shall be borne by the PURCHASER.

15.2. Where any deficiency has been observed during audit of the VENDOR on the risk parameters finalized by the PURCHASER or in the certification submitted by the Auditors, the VENDOR shall correct/resolve the same at the earliest and shall

provide all necessary documents related to resolution thereof and the auditor shall further certify in respect of resolution of the deficiencies. The resolution provided by the VENDOR shall require to be certified by the Auditors covering the respective risk parameters against which such deficiencies have been observed.

15.3. The VENDOR shall, whenever required by the PURCHASER, furnish all relevant information, records/data to the PURCHASER and/or auditors and/or inspecting officials of the PURCHASER/Reserve Bank of India and or any regulatory authority. The PURCHASER reserves the right to call and/or retain for any relevant material information/reports including auditor review reports undertaken by the VENDOR (e.g., financial, internal control and security reviews) and findings made on VENDOR in conjunction with the services provided to the PURCHASER.

16. BUSINESS CONTINUITY PLAN:

16.1. The service provider/vendor shall develop and establish a robust Business Continuity and Management of Disaster Recovery Plan if not already developed and established so as to ensure uninterrupted and continued services to the Bank and to ensure the agreed upon service level.

16.2. The service provider/vendor shall periodically test the Business Continuity and Management of Disaster Recovery Plan. The Bank may consider joint testing and recovery exercise with the Service provider/vendor.

17. CORRUPT AND FRAUDULENT PRACTICES:

17.1. Vendor/Service Provider shall at all times observe the highest standard of ethics during the entire contract period.

17.2. Vendor/Service Provider shall ensure compliance of CVC guidelines issued or to be issued from time to time for selection of vendor for Supply, Implementation, Migration and Support of the Solution by the Bank.

18. CONFIDENTIALITY AND NON-DISCLOSURE:

18.1. The vendor/service provider acknowledges and agrees that all tangible and intangible information obtained, developed or disclosed including all documents, data, papers, statements, any business / customer information, trade secrets and process of the Bank relating to its business practices in connection with the performance of services under this Agreement or otherwise, is deemed by the Bank and shall be considered to be confidential and proprietary information ("Confidential Information"), and shall not in any way disclose to anyone and the same shall be treated as the intellectual property of the Bank. The Service Provider shall ensure that the same is not used or permitted to be used in any manner incompatible inconsistent with that authorized procedure/ practice by the Bank. The Confidential Information will be safeguarded, and the Service Provider will take all necessary action to protect it against misuse, loss, destruction, alteration, or deletion thereof. Any violation of the same will be liable for action under the law.

18.2. VENDOR/ SERVICE PROVIDER shall take all necessary precautions to ensure that all confidential information is treated as confidential and not disclosed or used other than for the purpose of project execution. VENDOR/ SERVICE PROVIDER shall suitably defend, indemnify BANK for any loss/damage suffered by BANK on account of and to the extent of any disclosure of the confidential information.

18.3. No Media release/public announcement or any other reference to the Contract/RFP or any program there under shall be made without the written consent of the BANK, by photographic, electronic or other means.

18.4. Provided that the Confidentiality Clause may not be applied to the data or information which;

a) Was available in the public domain at the time of such disclosure through no wrongful act on the part of VENDOR/ SERVICE PROVIDER.
b) Is received by VENDOR/ SERVICE PROVIDER without the breach of this Agreement.
c) Is required by law or regulatory compliance to disclose to any third person.
d) Is explicitly approved for release by written authorization of the Bank.

18.5. Service Provider to ensure confidentiality of customer data and shall be liable in case of any breach of security and leakage of confidential customer related information

18.6. The vendor/service provider may disclose only the following types of data to the bank's customers and/or third parties with prior written consent of the bank: financial data, sensitive personal data, and other information explicitly permitted by the bank. All disclosures must comply with applicable laws, RBI regulations and guidelines. Prior written consent from the bank is required for any other disclosures, and detailed records of all shared data must be maintained by the service provider and shall be provided to the bank as and when required by the bank.

THESE CONFIDENTIALITY OBLIGATIONS SHALL SURVIVE THE TERMINATION OF THIS CONTRACT AND THE VENDOR/ SERVICE PROVIDER SHALL BE BOUND BY THE SAID OBLIGATIONS.

19. FORCE MAJEURE:

19.1. VENDOR/ SERVICE PROVIDER shall not be liable for default or non-performance of the obligations under the Contract, if such default or non-performance of the obligations under this Contract is caused by any reason or circumstances or occurrences beyond the control of VENDOR/ SERVICE PROVIDER, i.e. Force Majeure.

19.2. For the purpose of this clause, "Force Majeure" shall mean an event beyond the control of the VENDOR/ SERVICE PROVIDER, due to or as a result of or caused by acts of God, wars, insurrections, riots, earth quake and fire, Government policies or events not foreseeable but does not include any fault or negligence or carelessness on the part of the VENDOR/ SERVICE PROVIDER, resulting in such a situation.

19.3. In the event of any such intervening Force Majeure, VENDOR/ SERVICE PROVIDER shall notify the BANK in writing of such circumstances and the cause thereof immediately within seven days. Unless otherwise directed by the BANK, VENDOR/ SERVICE PROVIDER shall continue to perform / render / discharge other obligations as far as they can reasonably be attended / fulfilled and shall seek all reasonable alternative means for performance affected by the Event of Force Majeure.

19.4. In such a case, the time for performance shall be extended by a period (s) not less than the duration of such delay. If the duration of delay continues beyond a period of three months, the BANK and VENDOR/ SERVICE PROVIDER shall hold consultations with each other in an endeavour to find a solution to the problem. Notwithstanding above, the decision of the BANK shall be final and binding on the VENDOR/ SERVICE PROVIDER.

20. SOCIAL MEDIA POLICY:

20.1. No person of the Bank or the Vendor/Service Provider and third parties shall violate the Social Media Policy of the Bank.

20.2. The following acts on the part of personnel of the Bank or Vendor/Service Provider and third parties shall be construed as violation of Social Media Policy:

20.2.1. Non-adherence to the standards/guidelines in relation to Social Media Policy issued by the Bank from time to time.

20.2.2. Any omission or commission which exposes the Bank to actual or potential monetary loss or otherwise, reputation loss on account of non-adherence of Social Media related systems and procedures.

20.2.3. Any unauthorized use or disclosure of Bank's confidential information or data.

20.2.4. Any usage of information or data for purposes other than for Bank's normal business purposes and / or for any other illegal activities which may amount to violation of any law, regulation or reporting requirements of any law enforcement agency or government body.

21. HIRING OF BANK STAFF OR EX-STAFF:

The VENDOR/ SERVICE PROVIDER or subcontractor(s) shall not hire any of the existing/ ex/retired employee of the Bank during the contract period or after the closure/termination of contract even if existing/ ex/retired employee actively seek employment from the VENDOR/ SERVICE PROVIDER or sub-contractor(s). The period /duration after the date of resignation/ retirement/ termination after which the existing/ex/retired employee shall be eligible for taking up such employment shall be governed by regulatory guidelines/HR policies of the Bank

22. ADHERENCE TO BANKS IS SECURITY/CYBER SECURITY POLICIES:

22.1. VENDOR/ SERVICE PROVIDER shall comply with Bank's various policies like Information Security policy and Cyber Security Policy, Internet Policy, Information System Audit Policy, E-Mail policy and Guidelines.

22.2. In case of any security incident including but not limited to data breaches, denial of service, service unavailability, etc., the vendor/Service Provider shall immediately report such incident to the Bank.

23. PROTECTION OF DATA:

23.1. Vendor/Service Provider warrants that at all times, when delivering the Deliverables and/or providing the Services, use appropriate procedures and care to avoid loss or corruption of data. However, in the event that any loss or damage to Bank data occurs as a result of Vendor/Service provider's failure to perform its responsibilities in the RFP/ Gem Bid/ PO/Agreement, Vendor/Service Provider will at Bank's request correct or cause to be corrected any loss or damage to Bank data. Further, the cost of any corrective action in relation to data loss of any nature will be borne by Vendor/Service Provider, if such loss or damage was caused by any act or omission of Vendor/Service provider or its officers, employees, contractors or agents or other persons under Vendor/Service provider control.

23.2. Where the terms of the RFP/Gem Bid/PO/Agreement require any data to be maintained by the Bank, the Bank agrees to grant, Vendor/Service provider such access and assistance to such data and other materials as may be required by Vendor/Service Provider, for the purposes of correcting loss or damage to Bank data. If any data to be shared between the Bank and Vendor/Service provider for the purpose of the contract, the same shall be shared through secured

channels in an encrypted manner. The Vendor/ Service Provider shall process the relevant data at _____ (furnish the location). If the Vendor/ Service Provider proposes any change in data processing location, the same shall be notified to the Bank before the change of location. Vendor/Service provider is required to adhere to RBI guidelines for storage of data in India as per regulatory requirements/instructions, also to provide complete details of data captured, processed and stored, maintain confidentiality of the bank's and its customer's data and report same to the bank. The data if any to be stored by the vendor shall be stored in an encrypted manner. Vendor/Service provider will be liable to bank for any event for security breach and leakage of data/information. No biometric data shall be stored/ collected in the system associated with the vendor, unless allowed under extant statutory guidelines. The vendor shall have a structured process in place for secured removal/disposal/destruction of data and the details of the same shall be provided to the Bank as and when required by the bank.

23.3. Data privacy and security of the customer's personal information shared by the Bank shall always be ensured by Vendor/Service Provider. The personal information of customers shall not be stored and processed by the vendor except certain basic minimal data (viz. name, address, contact details of the customer etc.) as required for the performance of its obligations under this Agreement.

23.4. Vendor/Service Provider shall ensure compliance with all applicable law in relation to the services under this agreement and any modifications/changes in the applicable Law by Legislators and/or regulators during the currency of the agreement.

23.5. Vendor/Service Provider shall comply with all Data Protection Laws applicable in relation to the services under this agreement and shall ensure that any data provided by the Party under this Agreement is treated as confidential.

23.6. For the Purpose of this clause, "Data Protection Laws" means all directives, statutes, regulations, orders, decrees, decisions, or any other like legal instrument (whether enacted in India or any other relevant jurisdiction) which pertain to the protection of privacy and confidentiality of Personal Data including Digital Data Protection Act, 2023, Information Technology Act, 2000, and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, as amended from time to time

23.7. The Service provider shall ensure compliance with any modifications/changes in the applicable Law by Legislators and/or regulators during the currency of the contract and the contract shall be subject to the applicable law. If any modifications are required in existing applications/services due to change in the applicable Law by the Legislator and/or regulators, the Service provider shall make the necessary changes as per the instructions of the Bank. Payment terms for the modifications/changes necessitated due to change in applicable law shall be mutually agreed between the Bank and the Service provider. For this purpose "Applicable Law" means all the (a) applicable provisions of the constitution, treaties, statutes, laws (including the common law), codes, rules, regulations, ordinances, or orders of any Government Authority of India, Regulators; (b) orders, decisions, injunctions, judgments, awards, decrees, etc., of any Government Authority, Regulators including but not limited to rules, regulations, guidelines, circulars, Frequently Asked Questions (FAQs) and notifications issued by the RBI from time to lime; and (c) applicable international treaties, conventions and protocols that become enforceable from time to time.

24. DATA PROCESSING

Vendor/Service Provider shall comply with the Data Processing Terms and Conditions as furnished in Annexure-1 that complies with requirements of the current legal

framework in relation to data processing and with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) and any other data protection and privacy laws applicable to the Services, which shall form part and parcel of this agreement.

Once the provisions of the Digital Data Protection Act, 2023 are notified, Vendor/service Provider shall be required to execute an addendum to this agreement that complies with the legal provisions envisaged under the Digital Data Protection Act, 2023 and rules framed thereunder.

25. DISPUTE RESOLUTION MECHANISM:

All disputes and differences of any kind whatsoever, arising out of or in connection with this Contract or in discharge of any obligation arising under this Contract (whether during the course of execution of the order or after completion and whether beyond or after termination, abandonment or breach of the Agreement) shall be resolved amicably by negotiation between the parties. In case of failure to resolve the disputes and differences amicably through negotiation, the matter may be referred to mediation with the assistance of a mediator mutually agreed upon after issuance of at least 30 days' notice in writing to the other party clearly setting out the intention to refer such dispute to mediation. Proceedings of mediation shall be governed by The Mediation Act, 2023. Place of Mediation shall be Bengaluru, India . Proceedings of the mediation shall be conducted in English language.

26. GOVERNING LAWS AND JURISDICTION OF THE COURT:

All disputes and controversies between Bank and VENDOR/ SERVICE PROVIDER shall be subject to the exclusive jurisdiction of the courts in Bengaluru and the parties agree to submit themselves to the jurisdiction of such court as this Contract shall be governed by the laws of India.

27. NOTICES:

Any notice or other communication required or permitted by this Contract shall be in writing, in English, delivered by certified or registered mail, return receipt requested, postage prepaid and addressed as follows or to such other address as may be designated by notice being effective on the date received or, if mailed as set above:

If to BANK:

Registered Office Address: Canara Bank Head Office (Annex),
Centralized Procurement and Vendor Management Wing,
#14, M G Road, Naveen Complex,
Bengaluru -560001
Designated Contact Person: ..... (Designation)
Phone: 080-25599244
Email: **suppliermanagement@canarabank.com**

If to VENDOR/ SERVICE PROVIDER:

Registered Office Address:

Designated Contact Person: Sri. _____ (_____)
Phone: +91-_____
Email: _____

28. AMENDMENTS TO CONTRACT:

The terms and conditions of this Agreement may be modified by Parties by mutual agreement from time to time. No variation of or amendment to or waiver of any of the terms of this Agreement shall be effective and binding on the Parties unless evidenced in writing and signed by or on behalf of each of the Parties.

29. CONFLICT OF INTEREST:

29.1. VENDOR/ SERVICE PROVIDER represents and warrants that it has no business, professional, personal, or other interest, including, but not limited to, the representation of other clients, that would conflict in any manner or degree with the performance of its obligations under this Agreement.

29.2. VENDOR/ SERVICE PROVIDER represents and warrants that if any such actual or potential conflict of interest arises under this Agreement, Vendor/Service Provider shall immediately inform the Bank in writing of such conflict.

29.3. VENDOR/ SERVICE PROVIDER acknowledges that if, in the reasonable judgment of the Bank, such conflict poses a material conflict to and with the performance of VENDOR/ SERVICE PROVIDER's obligations under this Agreement, then the Bank may terminate the Agreement immediately upon Written notice to VENDOR/ SERVICE PROVIDER; such termination of the Agreement shall be effective upon the receipt of such notice by VENDOR/ SERVICE PROVIDER.

30. ESCALATION MATRIX:

The escalation matrix at the Vendor/Service Provider level, shall be provided as below.

In case of any issue with respect to the execution of the Project, Delivery of Hardware, Services etc., the Bank can escalate the issue as per the escalation matrix.

Escalation matrix shall be strictly followed to resolve any tickets, whenever raised.

Escalation Level	Name	Designation	Office Address	Mobile Number	Role & Responsibility	E-mail ID
First Level	---	---	---	---	---	---
Senior Level/Middle Level	---	---	---	---	---	---
Highest Level	---	---	---	---	---	---

31. GENERAL CONDITIONS TO CONTRACT:

31.1. The VENDOR/ SERVICE PROVIDER shall during the validity of this contract, provide access to all data, books, records, information, logs, alerts and business premises relevant to the service provided under this agreement to the Bank.

31.2. The VENDOR/ SERVICE PROVIDER shall adhere to RBI guidelines for storage of data in India as per regulatory requirements, also to provide complete details of data captured, processed and stored, maintain confidentiality of the bank's and its customer's data and report same to the bank, Vendor/Service Provider shall be liable to bank for any event for security breach and leakage of data/information

31.3. The VENDOR/ SERVICE PROVIDER shall abide/comply with applicable guidelines issued by RBI on Outsourcing of IT services vide master direction note no:RBI/2023-24/102 DoS.CO.CSITEG/SEC.1/31.01.015/2023-24 dated 10/04/2023 and its future amendments and communications.

31.4. No forbearance, indulgence, relaxation or inaction by any Party [BANK or VENDOR/ SERVICE PROVIDER] at any time to require the performance of any provision of Contract shall in any way affect, diminish, or prejudice the right of such Party to require the performance of that or any other provision of Contract.

31.5. No waiver or acquiescence of any breach, or any continuing or subsequent breach of any provision of Contract shall be construed as a waiver of any right under or arising out of Contract or an acquiescence to or recognition of any right and/or any position other than that expressly stipulated in the Contract.

31.6. All remedies of either BANK or VENDOR/ SERVICE PROVIDER under the Contract whether provided herein or conferred by statute, civil law, common law, custom, or trade usage, are cumulative and not alternative may be enforced successively or concurrently.

31.7. If any provision of Contract or the application thereof to any person or Party [BANK/ VENDOR/ SERVICE PROVIDER] is or becomes invalid or unenforceable or prohibited by law to any extent, this Contract shall be considered divisible as to such provision, and such provision alone shall be inoperative to such extent and the remainder of the Contract shall be valid and binding as though such provision had not been included. Further, the Parties [BANK and VENDOR/ SERVICE PROVIDER] shall endeavour to replace such invalid, unenforceable or illegal provision by one that is valid, enforceable, and legal and achieve substantially the same economic effect as the provision sought to be replaced.

31.8. None of the provisions of Contract shall be deemed to constitute a partnership between the Parties [BANK and VENDOR/ SERVICE PROVIDER] and neither Party [BANK nor VENDOR/ SERVICE PROVIDER] shall have any right or authority to bind the other as the other's agent or representative and no Party shall be deemed to be the agent of the other in any way.

31.9. Contract shall not be intended and shall not be construed to confer on any person other than the Parties [BANK and VENDOR/ SERVICE PROVIDER] hereto, any rights or remedies herein.

31.10. Contract shall be executed in English language in 1 (one) original, the BANK receiving the duly signed original and VENDOR/ SERVICE PROVIDER receiving the duly attested photocopy.

31.11. The vendor/service provider shall comply with all applicable provisions of the Information Technology Act, 2000 and any amendments thereto. This includes adhering to regulations and standards set forth under the Act concerning data protection.

31.12. The Vendor/Service Provider shall be liable for any loss caused to the bank due to any wilful negligence /malpractice by the Vendor/Service Provider or any of its officers, employees, agents or representatives which is found to be a

causative factor for any fraud, in spite of liability under the relevant statute, civil and/ or criminal as the case may be, for any malicious acts, negligent acts, wrongful acts, fraudulent acts and/ or offline transactions committed (including those committed by any of its employees, agents and/or representatives) in the performance of the Services under this Agreement and shall not be deemed to be acting on or behalf of the Bank in any manner whatsoever to the extent of such acts and/ or transactions.

31.13. Further Vendor/Service Provider the agrees that the guidelines issued by various regulators/government authorities/enforcement agencies etc. from time to time shall form part and parcel of this agreement and shall adhere to the same.

31.14. The Schedules and Annexures attached to this Agreement shall form and read as an integral part of this agreement and this agreement, the schedule, instruments, undertakings or otherwise executed presently or in future, herein contemplated to be entered into among, by or with the Parties hereto constitute the entire Agreement between the Parties.

IN **WITNESS** WHEREOF, the Parties hereto have executed this Agreement the day and year first herein above written.

Signature: Name: Designation: For & on behalf of: (BANK)	Signature: Name: Designation: For & on behalf of (VENDOR/ SERVICE PROVIDER)
In the presence of:	In the presence of:
Signature: 1: Name: Designation:	Signature: 1: Name: Designation:
Signature: 2:	Signature: 2:
Name: Designation:	Name: Designation:

Annexure-1

Data Processing Terms and Conditions

With respect to data processing the parties agree as follows:

1. **Definitions and Interpretation:**

1.1. Unless otherwise defined herein, terms and expressions used herein shall have the following meaning;

1.1.1. "Agreement" means the Contract Agreement with all schedules and Annexures.

1.1.2. "Controller" has the meaning given to "data controller" in the UK Data Protection Act 1998 and "controller" in the General Data Protection Regulation (as applicable).

1.1.3. "client" means a customer of Canara Bank.

1.1.4. "Data Protection Legislation" means as applicable, the UK Data Protection Act 1998, Directive 95/46/EC of the European Parliament and any laws or regulations implementing it, the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and any equivalent or replacement law in the UK and any other data protection and privacy laws applicable to the Services.

1.1.5. "Data subject" has the meaning given to it in the Data Protection Legislation.

1.1.6. "Personal Data" has the meaning given to it in the Data Protection Legislation and relates only to the Personal Data processed by a Contracted Processor on behalf of Canara Bank pursuant to or in connection with the Agreement in relation to the Services provided.

1.1.7. "Processor" means a data processor providing service to Canara Bank.

1.1.8. "Subprocessor" means any person appointed by or on behalf of processor to process personal Data on behalf of Canara Bank in connection with the Agreement.

1.1.9. "Data Protection Laws" means EU Data Protection Laws and, to the extent applicable, the data protector or privacy laws of any other country.

1.1.10. "EEA" means the European Economic Area.

1.1.11. "EU Data Protection Laws" means EU Directive 95/46/EU, as transported into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR.

1.1.12. "GDPR" means EU General Data Protection Regulation 2016/679.

1.1.13. "Data Transfer" means:

1.1.13.1. a transfer of Personal Data from Canara Bank to a processor; or

1.1.13.2. an onward transfer of Personal Data from a Processor to a Subcontracted Processor, or between two establishments of a Processor in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreement put in place to address the data transfer restrictions of Data Protection Laws).

1.1.14. "Services" means the services to be performed by the Processor in the Agreement (as provided in Schedule 1).

1.1.15. "Supervisory authority" has the meaning given to it in the Data Protection Legislation.

1.1.16. "Personal data breach" has the meaning given to it in the Data Protection Legislation.

1.1.17. "Personnel" means the personnel of the Processor, Sub processors who provided the applicable Services; and

1.1.18. "Terms and Conditions" means the terms and conditions contained herein for the purpose of Data processing.

1.1.19. "Third country" has the meaning given to it in the Data Protection Legislation.

Processing of Personal Data:

1.2. In the course of providing Services to Canara Bank, the Processor may Process Personal Data on behalf of Canara Bank.

1.3. Processor shall:

1.3.1. comply with all applicable Data Protection Laws in the Processing of Personal Data; and

1.3.2. not Process Personal Data other than on the relevant documented instructions of Canara Bank.

2. PROCESSOR OBLIGATIONS:

2.1. Processor Personnel:

Processor shall take reasonable steps to ensure the reliability of any employee, agent or sub-processor who may have access to Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Personal Data, as strictly necessary for the purposes of the Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

2.1.1. The Processor shall process Personal Data only on the documented instructions from Canara Bank from time to time. Canara Bank shall notify the Processor of any amendments to existing instructions or additional instructions in relation to the processing of Personal Data in writing and Processor shall promptly comply with such instructions.

2.1.2. Notwithstanding clause 3.1, the Processor (and its Personnel) may process the Personal Data if it is required to do so by European Union law, Member State law or to satisfy any other legal obligations to which it is subject. In Such circumstance, the Processor shall notify Canara Bank of that requirement before it processes Personal Data, unless the applicable law prohibits it from doing so.

2.1.3. The Processor shall immediately notify Canara Bank if, in opinion, Canara Bank's documented data processing instructions breach the Data Protection Legislation. If and to the extent the Processor is unable to comply with any instruction received from Canara Bank, it shall promptly notify Canara Bank accordingly.

2.1.4. The purpose of the Processor Processing Personal Data is the performance of the Services pursuant to the Agreement.

2.2. Security:

2.2.1. Taking into account the nature, scope, context and purposes of Processing (provided in **Schedule 2**) as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall in relation to Personal Data implement appropriate technical and organizational measures (Processor obligations in **Schedule 3**) to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

2.2.2. In assessing the appropriate level of security, Processor shall take into account, in particular, risks related to processing of Personal Data.

2.2.3. The Processor shall use appropriate technical and organisational measures to prevent the unauthorised or unlawful processing of Personal Data and protect against accidental loss or destruction of, or damage to, any Personal Data during processing activities. It shall implement and maintain the security safeguards and standards based on the IS policy of Canara Bank as updated and notified to the Processor by Canara Bank from time to time. The Processor will not decrease the overall level of security safeguards and standards during the term of Agreement without Canara Bank's prior consent.

2.3. Sub-Processing:

2.3.1. The Processor shall not appoint (or disclose any Personal Data to) any Sub-Processors without prior written authorisation from Canara Bank. The Processor shall provide Canara Bank with (no less than xx days) prior written (including email) notice before engaging a new Sub processor thereby giving Canara Bank an opportunity to object to such changes. If Canara Bank wishes to object to such new Sub processor, then Canara Bank may terminate the relevant Services without penalty by providing written notice of termination which includes an explanation of the reasons for such obligation.

2.3.2. The processor shall include in any contract with its Sub processor who will process Personal Data on Canara Bank's behalf, obligations on such Sub processors which are no less onerous than those obligations imposed upon the Processor in this Agreement relating to Personal Data. The Processor shall be liable for the acts and omissions of its Sub processors to the same extent to which the processor would be liable if performing the services of each Sub processor directly under the terms of the Agreement.

2.4. Data subject Rights:

Data subjects (Canara Bank NRI customers) whose personal data is processed pursuant to the Agreement have the right to request access to and the correction, deletion or blocking of such personal data under Data Protection Legislation. Such requests shall be addressed to and be considered by Canara Bank responsible for ensuring such requests are handled in accordance with Data Protection Legislation.

2.4.1. Taking into account the nature of the Processing, Processor shall assist Canara Bank by implementing appropriate technical and organisational measures (Processor Obligations in Schedule **3**), insofar as this is possible, for the fulfilment of Canara Bank's obligations, as reasonably understood by Canara Bank to respond to requests to exercise Data Subject rights under the Data Protection Laws.

2.4.2. In case Data Subject Requests are received by Processor, then the Processor shall:

2.4.2.1. promptly notify Canara Bank if it receives a request from a Data Subject under any Data Protection Law in respect of Personal Data; and

2.4.2.2. ensure that it does not respond to that request except on the documented instructions of Canara Bank or as required by Applicable Laws to which the Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws

2.4.2.3. inform Canara Bank of that legal requirement before the Processor responds to the request.

2.5. Personal Data Breach:

2.5.1. Processor shall notify Canara Bank without undue delay upon Processor becoming aware of a Personal Data Breach affecting Personal Data, providing Canara Bank with sufficient information to allow Canara Bank to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

2.5.2. Processor shall co-operate with Canara Bank and take reasonable commercial steps as are directed by Canara Bank to assist in the investigation mitigation and remediation of each such Personal Data Breach.

2.6. Data Protection Impact Assessment and Prior Consultation:

Processor shall provide reasonable assistance to Canara Bank with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Canara Bank reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Personal Data by and taking into account information available to, the Processors.

2.7. Deletion or return of Personal Data:

2.7.1. Subject to this section 3.7 Processor shall, promptly and in any event within <xx>
business days of the date of cessation of any Services involving the Processing of Personal Data (the "Cessation Date"), delete all copies of those Personal Data.

2.7.2. Processor shall provide written certification to Canara Bank that it has section3.7 within <xx> business days of the Cessation Date.

2.8. Audit Rights:

The Processor shall make available to Canara Bank and any supervisory authority or their representatives the information necessary to demonstrate its compliance with this Terms and Conditions and allow for and contribute to audits and inspections by allowing Canara Bank , its clients, a supervisory authority or their representatives to conduct an audit or inspection of that part of the Processor's business which is relevant to the Services { on at least an annual basis (or more frequently when mandated by a relevant supervisory authority or to comply with the Data Protection Legislation)and} on reasonable notice, in relation to the Processing of Personal Data by the Processor.

2.9. Data Transfer:

The Processor may not transfer or authorize the transfer of Data to countries outside the EU/India and /or the European Economic Area (EEA) without the prior written consent of Canara Bank. If personal data processed under the agreement is transferred from a country within the European Economic Area to a country outside the European Economic Area, the Parties shall ensure that the personal Data are adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on EU approved standard contractual clauses/ EU-US Privacy Shield for the transfer of personal data.

2.10. Records:

The Processor shall maintain written records of its data processing activities pursuant to providing the Services to Canara Bank in accordance with Data Protection Legislation.

2.11. Notify:

The Processor shall immediately and fully notify Canara Bank in writing of any communications the Processor (or any or its Sub processors) receives from third parties in connection with the processing of the Personal Data, including (without limitation) subject access requests or other requests, notices or other communications from individuals, or their representatives, or from the European Data Protection Board, the UK's Information Commissioner's Office (in the case of the United Kingdom) and/or any other supervisory authority or data protection authority or any other regulator (including a financial regulator)or court.

2.12. Agreement Termination:

Upon expiry or termination of the Agreement or the Services for any reason or Canara Bank's earlier request, the Processor shall: (i) return to Canara Bank and (ii) delete from all computer systems and other data storage systems, all Personal Data, provided that the Processor shall not be required to return or delete all or part of the Personal Data that it is legally permitted to retain. The Processor shall confirm to Canara Bank that it has Complied with its obligation to delete Personal Data under this clause.

3. CANARA BANK'S OBLIGATIONS:

Canara Bank shall:

3.1. in its use of the services, process the Personal Data in accordance with the requirements of the Data Protection Legislation.

3.2. use its reasonable endeavours to promptly notify the Processor if it becomes aware of any breaches or of other irregularities with the requirements of the Data Protection Legislation in respect of the Personal Data processed by the Processor.

Schedule-1

1.1.Services

<<Insert a description of the Services provided by the Data Processor (under the Principle Service Agreement, where relevant)>>.

Schedule-2

Personal Data

Category of Personal data	Category of Data subject	Nature of Processing carried out	Purpose of processing	Duration of Processing

SCHEDULE 3

Technical and Organisational Data Protection Measures

1. The Processor shall ensure that, in respect of all Personal Data it receives from or processes on behalf of CANARA BANK, it maintains security measures to a standard appropriate to:

   1.1. the nature of the Personal Data; and
   1.2. Safeguard from the harm that might result from unlawful or unauthorised processing or accidental loss, damage, or destruction of the Personal Data.

2. In particular, the Processor shall:
   2.1. have in place, and comply with, a security policy which:
      2.1.1. defines security needs based on a risk assessment.
      2.1.2. allocates responsibility for implementing the policy to a specific individual (such as the Processor's Data Protection Officer) or personnel and is provided to CANARA BANK on or before the commencement of this Agreement.
      2.1.3. ensure that appropriate security safeguards and virus protection are in place to protect the hardware and software which is used in processing the Personal Data in accordance with best industry practice.
      2.1.4. prevent unauthorised access to the Personal Data.
      2.1.5. protect the Personal Data using pseudonymisation and encryption.
      2.1.6. ensure the confidentiality, integrity and availability of the systems and services in regard to the processing of Personal Data.
      2.1.7. ensure the fast availability of and access to Personal Data in the event of a physical or technical incident.
      2.1.8. have in place a procedure for periodically reviewing and evaluating the effectiveness of the technical and organisational measures taken to ensure the safety of the processing of Personal Data.
      2.1.9. ensure that its storage of Personal Data conforms with best industry practice such that the media on which Personal Data is recorded (including paper records and records stored electronically) are stored in secure locations and access by personnel to Personal Data is strictly monitored and controlled.
      2.1.10. have secure methods in place for the transfer of Personal Data whether in physical form (for example, by using couriers rather than post) or electronic form (for example, by using encryption).
      2.1.11. password protect all computers and other devices on which Personal Data is stored, ensuring that all passwords are secure, and that passwords are not shared under any circumstances.
      2.1.12. not allow the storage of the Personal Data on any mobile devices such as laptops or tablets unless such devices are kept on its premises at all times.
      2.1.13. take reasonable steps to ensure the reliability of personnel who have access to the Personal Data.
      2.1.14. have in place methods for detecting and dealing with breaches of security (including loss, damage, or destruction of Personal Data) including:
         2.1.14.1. having a proper procedure in place for investigating and remedying breaches of the GDPR; and
         2.1.14.2. notifying CANARA BANK as soon as any such security breach occurs
      2.1.15. have a secure procedure for backing up all Personal Data and storing back-ups separately from originals; and
      2.1.16. adopt such organisational, operational, and technological processes and

procedures as are required to comply with the requirements of ISO 27001:2013 and CANARA BANK's Information Security Policy and other related policies/guidelines as appropriate.