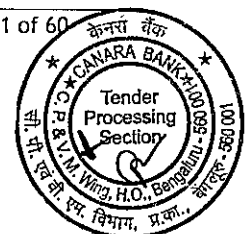


Corrigendum-3 to GeM Bid ref. no: GEM/2025/B/5781717 dated 04/01/2025 for Selection of Service Provider for Supply, Installation, Implementation, Integration, Customization and Maintenance of Document Management Solution for Global Trade Processing Centre for a period of five years in Canara Bank.

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

a.

Sl No	Section/ Annexure/ Appendix of GeM Bid	Clause No.	Existing Clause	Amended Clause
1.	Section C - Deliverable And Service Level Agreements	1. Project Timelines	1.4.4.Delivery of Perpetual Enterprise Licenses for Document Management Solution for Global Trade.Processing Centre: Bidder has to deliver the Licence within Four (4) weeks from the date of Installation, Integration and Commissioning of Hardware & Other Items (including OS) at DC, DRC & UAT Locations.	<u>1.4.4. Delivery, Installation, Integration, Commissioning of Perpetual Enterprise License and Setting up the Base version of proposed Document Management Solution</u> for Global Trade Processing Centre: Bidder has to deliver the Licence within Four (4) weeks from the date of Installation, Integration and Commissioning of Hardware & Other Items (including OS) at DC, DRC & UAT Locations.
2.	Section C - Deliverable And Service Level Agreements	5.Payment Terms	Existing Payment Terms	<u>Amended Payment Terms Attached to this Corrigendum</u>
3.	Section C - Deliverable And Service Level Agreements	7.Penalties/ Liquidated Damages	7.2.1.Non-compliance of the delivery of Enterprise Licenses for Document Management Solution for Global Trade Processing Centre per clause 1.4.4 will result in imposing penalty of 0.50% of the total cost of Document Management Solution for Global Trade Processing Centre on delay in delivery per week or part thereof by the Bank as per Table-B of Annexure-17.	7.2.1.Non-compliance of the delivery of Enterprise Licenses for Document Management Solution for Global Trade Processing Centre per clause 1.4.4 will result in imposing penalty of 0.50% of the <u>total cost of Perpetual Enterprise License</u> for Document Management Solution for Global Trade Processing Centre on delay in delivery per week or part thereof by the Bank as per Table-B of Annexure-17.
4.	Annexure-2 Pre-Qualification Criteria	Annexure-2 Pre-Qualification Criteria	Existing Annexure-2 Pre-Qualification Criteria	<u>Amended Annexure-2 Pre-Qualification Criteria Attached to this Corrigendum</u>

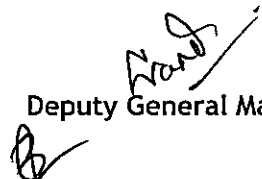


5.	Annexure-3 Bidder's Profile	Annexure-3 Bidder's Profile	5. Proposed Document Management Solution for Global Trade Processing Centre Solution	<u>5. Name of commercial banks where solution is deployed for similar purpose.</u>
6.	Annexure-8 Scope of Work	Annexure-8 Scope of Work	Existing Scope of Work	<u>Amended Scope of Work Attached to this Corrigendum</u>
7.	Annexure-8 (A) Sizing of Hardware including Software/OS for UAT, DC & DRC	Annexure-8 (A) Sizing of Hardware including Software/OS for UAT, DC & DRC	Existing Annexure-8 (A) Sizing of Hardware including Software/OS for UAT, DC & DRC	<u>Amended Annexure-8 (A) Sizing of Hardware including Software/OS for UAT, DC & DRC Attached to this Corrigendum</u>
8.	Annexure-17 Bill of Material	Annexure-17 Bill of Material	Existing Annexure-17 Bill of Material	<u>Amended Annexure-17 Bill of Material Attached to this Corrigendum</u>
9.	Appendix-G	Draft Contract Agreement	Existing Draft Contract Agreement	<u>Amended Draft Contract Agreement attached with this Corrigendum</u>

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

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

Date: 07/02/2025
Place: Bengaluru


Deputy General Manager

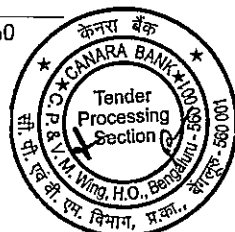




5. Payment Terms

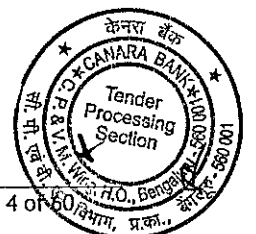
5.1 The payment schedule will be as under and will release after execution of contract agreement:

Sl. No.	Payment Stages	% of Payment	Condition/Remarks
1.	Hardware cost (including OS)	70% as per Table-A of Annexure- 17	On delivery and commissioning of Hardware and required Software items for the setup of infrastructure for the proposed solution and on submission of Invoice and Acceptance/Sign off by the Bank and after deducting Liquidated Damages (if Any) and on production of relevant documents.
		20% as per Table-A of Annexure- 17	On successful go-live of the proposed solution and on submission of Invoice and Acceptance/Sign off by the Bank and after deducting Liquidated Damages (if Any) and on production of relevant documents.
		10% as per Table-A of Annexure- 17	On completion of warranty or on submission of BG for the equivalent amount and after deducting Liquidated Damages (if Any).
2.	Perpetual Enterprise License cost	50% as per Table-B of Annexure- 17	<u>On delivery, Installation, Integration, Commissioning of Perpetual Enterprise License and Setting up the Base version of proposed Document Management Solution and on production of relevant documents like delivery signoff and invoice of the items supplied duly approved by the Bank Officials while claiming the payment.</u>
		50% as per Table-B of Annexure- 17	<u>On successful implementation and go live of all modules of Proposed solution. Payment will be released after deducting applicable penalties and Liquidated damages as per GeM Terms and on submission of Invoice, Acceptance/Sign off by the Bank and on production of relevant documents.</u>
3.	One time implementation cost	30% as per Table-C of Annexure- 17	On successful implementation in UAT and on submission of Invoice and Acceptance/Sign off by the Bank on production of relevant documents and after deducting Liquidated Damages (if Any).
		50% as per Table-C of Annexure- 17	On successful implementation in DC, DR and go-live and on submission of Invoice and Acceptance/Sign off by the Bank on production of relevant documents and after deducting Liquidated Damages (if Any).



		10% as per Table-C of Annexure-17	On successful completion of DR Drill and on submission of Invoice and Acceptance/Sign off by the Bank on production of relevant documents and after deducting Liquidated Damages (if Any).
		10% as per Table-C of Annexure-17	On successful completion of Migration and on submission of Invoice and Acceptance/Sign off by the Bank on production of relevant documents and after deducting Liquidated Damages (if Any).
4.	AMC/ATS (as per Table-D of Annexure-17.)	Payment will be made Quarterly in arrears after deducting applicable penalties and Liquidated damages.	
5.	Additional requirements/ additional customization/ enhancement (as per Table-F of Annexure-17)	100% payment will be released after Successful Go Live and on production of relevant documents and after deducting Liquidated Damages (if Any)	
6.	Dedicated Onsite Resources	Payment will be Monthly in arrears as per Table-E of Annexure-17 after deducting applicable penalties and Liquidated damages (if Any).	

- 5.2 Bank will release the payment on completion of activity and on production of relevant documents/invoices. Please note that Originals of invoices (plus One Copy) reflecting GST, GSTIN, State Code, HSN Code, State Name, Taxes & Duties, Proof of delivery duly signed by Bank officials of the respective Branch/office and Manufacturer's / Supplier's Warranty Certificate should be submitted while claiming payment in respect of orders placed.
- 5.3 The selected bidder has to submit installation report/Sign off report duly signed by the Bank officials of the respective Branch/offices in originals while claiming payment. The invoice and installation report should contain the product serial number of the items supplied.
- 5.4 Bank will not pay any amount in advance unless otherwise specified in this RFP.
- 5.5 Payment shall be released within 30 days from the date of submission of relevant documents as per RFP terms.
- 5.6 The Bank shall finalize the installation and acceptance format mutually agreed by the selected bidder. The selected bidder shall strictly follow the mutually agreed format and submit the same for each location wise while claiming installation and acceptance payment.
- 5.7 The payments will be released through NEFT / RTGS after deducting the application LD/Penalty, TDS if any, by centrally by Head Office at Bengaluru and the selected bidder has to provide necessary Bank Details like Account No., Bank's Name with Branch, IFSC Code etc.





**Amended Annexure-2
Pre-Qualification Criteria**

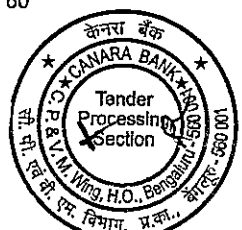
(Should be submitted on Company's letter head with company seal and signature of the authorized person)

SUB: RFP for Selection of Service Provider for Supply, Installation, Implementation, Integration, Customization and Maintenance of Document Management Solution for Global Trade Processing Centre for a period of five years in Canara Bank

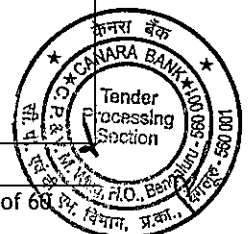
Ref: GEM/2025/B/5781717 dated 04/01/2025

We have carefully gone through the contents of the above referred RFP along with replies to pre-bid queries & amendment, if any and furnish the following information relating to Pre-Qualification Criteria.

Sl. No.	Qualification Criteria	Documents to be submitted In compliance with Qualification Criteria	Bidders Response
1.	Signing of Pre-Contract Integrity Pact	The bidder should submit signed Pre-Contract integrity pact on Non-Judicial Stamp Paper of Rs.500/- or more (as per respective state Stamp Act whichever is higher) as per Appendix-F.	
2.	The Bidder should either be Class-I or Class-II local supplier as defined in Public Procurement (Preference to Make in India) Revised Order (English) dated 19/07/2024.	Certificate of local content to be submitted as per Annexure-5 as applicable.	
3.	<p>The Company operating should be legally compliant company and can be:</p> <p>a. A partnership firm or a Limited Liability Partnership duly registered under the Limited Liability Partnership Act, 2008. (OR)</p> <p>b. Company duly registered in India as per Indian Companies Act, 1956 or Indian Companies Act, 2013. (OR)</p> <p>c. Proprietorship firm duly registered under the applicable shops and commercial Establishments Act and should be compliant to all the applicable laws.</p>	<p>Copy of Certificate of FIRM/LLP registration. (OR)</p> <p>Copy of Certificate of Incorporation and Certificate of Commencement of business in case of Public Limited Company or Certificate of Incorporation in case of Private Limited Company, issued by the Registrar of Companies.</p> <p>(OR)</p> <p>Copy of Certificate of registration under and Certificate of Commencement of business in case of Public Limited Company or Certificate of Incorporation in case of Private Limited Company, issued by the Registrar of Companies.</p> <p>For (c) Documentary proof for confirming registration of Proprietorship firm (e.g. Copy of Certificate of</p>	



Sl. No.	Qualification Criteria	Documents to be submitted In compliance with Qualification Criteria	Bidders Response
		registration under shops and commercial Establishments Act., GST etc.)	
4.	If not a group of company, Bidder Company shall not be owned or controlled by any Director, or Key managerial personnel of the Canara Bank or their relatives.	Letter of Undertaking in company's letter head has to submit in this effect.	
5.	The bidder should provide confirmation that any person/ Partnership/ LLP/ Company including any subsidiary or holding company/ proprietorship connected to bidder directly or indirectly has not participated in the bid process.	The bidder should submit letter of confirmation on the Company's letter head to this effect.	
6.	The bidder should have an average annual turnover of Rs.40 Crores during last 3 financial years (i.e., 2021-22 & 2022-23, 2023-24) from Indian operations. This must be the individual company turnover and not of any group of companies.	Bidder should submit Audited Balance Sheet copies for last 3 financial years i.e., 2021-22 & 2022-23, 2023-24 along with certificate from the Company's Chartered Accountant to this effect with Unique Document Identification Number.	
7.	<u>The Bidder/OEM should have implemented/maintaining the Trade Finance Solution in at least one of the Scheduled Commercial Banks in India having more than 1000 branches or the solution handling at least 20000 Branch users/sessions during last five years as on the date of submission of bid</u>	<u>The bidder/OEM has to provide relevant purchase order/work order / engagement letter & signoff along with satisfactory project completion certificate/ Reference letter from the Concerned Organization/ Email reference from the client detailing the services along with Name, Designation, Contact details.</u>	
8.	The Net Worth of bidder should not be negative as on 31/03/2024 and also should have not been eroded more than 30% in the last three financial years ending on 31/03/2024.	The bidder should submit certificate from the Company's Chartered Accountant with UDIN to this effect.	
9.	Any bidder (including OEM and OSD/OSO, if any) from a country which shares a land border with India will be eligible to bid, only if the bidder (including OEM and OSD/OSO) are registered with the Competent Authority. Bidder (entity) from a country which shares a land border with India means: a. An entity incorporated, established or registered in such a country; or	A declaration stating "We have read the clause regarding restrictions on procurement from a bidder of a country which shares a land border with India. We further certify that we and our OEM are not from such a country or if from such a country, has been registered with Competent Authority. We hereby certify that we and our OEM fulfills all requirements in this regard and are eligible to be considered" to be submitted in Company's letter head.	



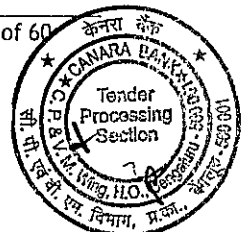


Sl. No.	Qualification Criteria	Documents to be submitted In compliance with Qualification Criteria	Bidders Response
-	b. A subsidiary of an entity incorporated, established or registered in such a country; or c. An entity substantially controlled through entities incorporated, established or registered in such a country; or d. An entity whose beneficial owner is situated in such a country; or e. An Indian (or other) agent of such an entity; or f. A natural person who is a citizen of such a country; or g. A consortium or joint venture where any member of the consortium or joint venture falls under any of the above.	[Where applicable, evidence of valid registration by the Competent Authority shall be attached.]	
10.	Bidders should not be under debarment/blacklist period for breach of contract/fraud/corrupt practices by any Scheduled Commercial Bank/ Public Sector Undertaking / State or Central Government or their agencies/ departments as on date of submission of bid.	The bidder should submit self-declaration on the Company's letter head to this effect.	
11.	The <u>bidder/OEM</u> should have support office for 24x7 support.	The Bidder should submit the details viz., address, phone no., email id and contact person Name & Mobile no. etc.,	
12.	Authorization Certificate - Whether the Bid is authenticated by authorized person.	Bidder to submit a copy of the Board Resolution and the Power of Attorney and KYC documents evidencing the authority delegated to the authorized signatory.	

We confirm that the information furnished above is true and correct. We also note that, if there are any inconsistencies in the information furnished above, the bid is liable for rejection. All documentary evidence/certificates confirming compliance to Pre-Qualification Criteria should be part of the RFP.

Date:
Place:

Signature with seal
Name:
Designation :



Annexure-8

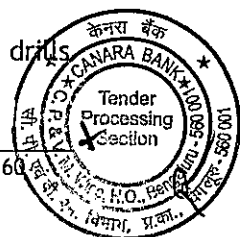
Scope of Work

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

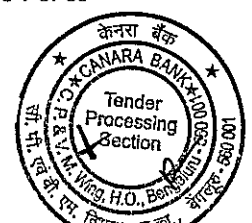
SUB: RFP for Selection of Service Provider for Supply, Installation, Implementation, Integration, Customization and Maintenance of Document Management Solution for Global Trade Processing Centre for a period of five years in Canara Bank

Ref: GEM/2025/B/5781717 dated 04/01/2025

1. The Bidder Shall Supply, provide Installation, Implementation, Integration, Customization and Maintenance of a software application for "Document Management Solution - Trade Finance" herein after referred to as "application", for "Canara Bank" herein after referred to as "Bank", during the contract period as per the requirement given in this RFP.
2. The Application will be a front end facility for Branches & customers to upload and forward Trade finance, Forex, Inland & related transaction documents, place requests, submit forms etc. The Application will back end facility for the centralized processing center users. Basically, it will be an exclusive document management solution for Trade Finance facilitating the Bank's existing "Trade finance Solution Package" which is Core Banking Solution (CBS)ss. The proposed application should provide platform to punch in all Forex & Inland Trade transactions, Remittances and provide facility to upload transaction related scanned documents from branches and customers. The application must be web based between branches, customers and centralized processing center establishing highly secured, encrypted sessions.
3. Application for branches should able to handle minimum concurrent session of 1000 and customer application should handle minimum concurrent session of 500.
4. The Bank is having pan India presence of more than 9658 branches/offices spread across Bank's Circles and Regions .The proposed application should scalable to handle all session request from all bank branches including the centralized processing centres.
5. Bidder has to provide end to end solution along with necessary hardware and licenses for the Implementation of the proposed application and the Bidder must provide the required specifications as per Annexure-8 (A).
6. The Application (front end) for branch/offices/customers/International Branches/ GIFT City users, must have the modules/ functionalities as listed in Annexure-9 which are deliverables. under this RFP.
7. The Application must have in built feature of enabling/disabling modules/functions/pages/forms etc by admins for end users such as branches/offices/customers.
8. Application should support High availability in production & DR environments. The architecture must ensure uninterrupted service even during failures or upgrades.
9. The Infrastructure at Each Site (DC & DR) shall be configured in High Availability with either Active-Active or Active-Passive configuration as supported by the solution architecture.
10. DC & DR Sites should be in Active-Passive Configuration .
11. The Bidder should comply with DPDP (Digital personal data protection) act and subsequent amendment issued by Govt.Of India.
12. The bidder should arrange qualified resources during all planned and unplanned DR drills during contract period.

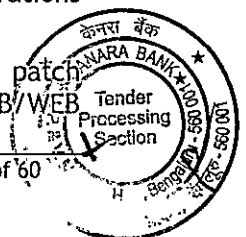


13. The Bidder has to study the requirements of the application for the installation in Bank's DC & DRC setup and prepare implementation plan accordingly. On approval of the same by the Bank, installation and configuration to be carried out.
14. The Solution must be capable of supporting LDAP and system can be integrated with Windows Active Directory (AD) to achieve Single Sign on (SSO).
15. The Bidder is required to maintain the RTO and RPO as per the Bank's Business Continuity Policy. For the application, maximum RTO of 3 hours and RPO 15 minutes should be maintained. Application should support syncing of documents to DR site for BCP purpose and should be available while DR Drill and other contingencies while running application from another site.
16. The Application should be compatible with an operating system having features like multi-tasking, multi-user support, timesharing, dynamic memory management, I/O spooling, multi-level security, system logging, error analysis, and recovery. The Application must be compatible with system components such as hardware, software, network etc.
17. The Application should possess robust scalable architecture with efficient design and architecture such as Client-Server model with edge computing, that is with Maximized local processing & Minimized Server interaction, reduced latency, Optimized bandwidth and hence scalable horizontally and vertically. The Application should be capable/scalable to take care of future needs/ requirements to align with CBS, loan processing, trade finance, HRMS integration, MIS, Data warehousing, SAS etc. (Capability to build two way Interfaces to be ensured), which supports modular upgrades without disrupting core functionalities.
18. The Bidder shall provide one Production License (DC & DR) and one testing environment (UAT).
19. The Application should be capable to scan, store, index, search, retrieve, and transmit images/documents/data from the respective scanning center/branch/customer portal, etc. (front end) to centralized processing center (back end). The Bidder Shall Supply, install & provide configuration of necessary scanning software. The application should be capable of supporting upload of scanned/electronic documents/files in digital form from Bank provided scanner or any related applications. The application involves Image capturing in a hybrid environment/storage/data entry/ i.e. distributed as well as in central processing environment Workflow based.
20. The centralized processing center must have access to the data and can download the uploaded documents for verification and able to add/modify/delete certain data and can approve/reject/hold the transaction as the case may be. Further, if the transaction is approved by the accounting user in the application, transaction can be pushed to CBS with creation of contract in CBS under Hold status. On accounting completion, the CBS contract parameters need to be flown back to the application.
21. Application should be efficient enough to do optimal space management (log management & archiving, binary management etc.) & document compression without compromising quality and legitimacy. The application should be capable of Auto Crunch of scanned documents at client level to reduce the file size instead of rejecting the heavy scanned documents. The application should be configurable to the different types of scanners to directly scan the documents into the application.
22. The Application architecture should include provisions for real time monitoring and automatic alerts for system health, performance, security and any issues.
23. The Application architecture must establish encrypted communication between client & server that is secured session management; the architecture must also ensure data encryption (at rest and in transit), enhanced prevention of web vulnerabilities, secured API end points, implementation of web application firewalls, Unique IP Assignment for enhanced Security & accountability etc. The application must comprehensively comply with latest



Information security standards of ISO; presently ISO/IEC 27001:2022 or above as and when standards updated.

24. The Bidder shall implement document security plan conforming to the regulatory security guidelines in vogue and also during entire contract period at no additional cost to the Bank.
25. After implementation of the application in production environment, within 3 months of time the bidder must complete the application security audit as per Bank policy through reputed Auditors with any additional cost to Bank.
26. The bidder has to comply the observations made during VAPT, RBI audit or by any internal/external audits and close the remarks within stipulated timeline .
27. The Application must provide seamless migration of legacy data from Bank's existing DMS (Document Management Solution) and ensure availability/accessibility of all legacy data from the proposed new application.
28. The application should support continuous integration/continuous deployment to allow for regular, automated testing and deployment of updates or new versions, ensuring that updates are deployed rapidly with minimal risk keeping the application software up-to-date with latest features, security patches etc. The application should be backward compatible with previous versions without any downtime to production environment. The bidder has to apply new release/Bug fix/upgrade/update during project tenure without any additional cost. Comprehensive Support to be provided by vendor for all application instances in UAT, Production & DR environment.
29. The application must support deployment across the Bank's work locations & departments, offering core functionalities with the option for tailored customizations. For instance: Implementation of the application for remittance module exclusively at Canara Bank, IFSC Branch, GIFT city. Bidder should factor sufficient licences (without any additional cost to Bank) for Banks official setups like Branch/office, GIFT City, International Offices, Customers etc.
30. The bidder shall ensure presence of 1 senior onsite resource & 1 junior onsite resource on all working days and the bidder will be required to provide backup resource in case of unavailability of onsite resource, at Bank identified location anywhere in India. Bank may change the project / support location at any time during the contract period and the bidder shall ensure availability of resources on bank decided such changed locations without any additional cost to the Bank. The onsite resources should be the on roll employees of the bidder. The brief scope for the onsite resource is as follows:
 - a) The senior onsite resource shall have minimum 5 years of domain knowledge and the junior onsite resource shall have 2 years of domain knowledge and experience of handling / maintaining the proposed application respectively.
 - b) The both onsite resources at present required to depute at Canara Bank, Manipal office. However, in future the deputation of onsite resource may placed any where in India .The bidder has to provide onsite resource unconditionally.
 - c) The L2 & L1 resource should be minimum B.E/B.Tech (Bachelors of Engineer/technologies).
 - d) The onsite resource will provide support to the deployed Solution including DBA activity of bidder's system for the entire contract period.
 - e) The onsite resource shall be responsible for maintaining the system and application uptime as specified by the Bank.
 - f) The onsite resource should have knowledge of Database and related Operations required for maintaining the uptime of the solution.
 - g) The onsite resource should perform the Backup/restoration/ patch /updates/upgrades of related activities pertaining to the OS/APP/DB/WEB



/Middleware/ Servers and related peripherals of proposed application and related servers.

- h) The onsite resource shall be responsible for log shipment, backup, DC/DR switchover drill, restore-implementation of disaster recovery plan, if required as advised by the Bank.
- i) The onsite resource shall work as per standard operating processes defined by the Bank.
- j) The onsite resource shall follow and implement change management process as per the Bank guidelines/policies.
- k) The onsite resource shall maintain log of all down calls for MIS purpose and provide required MIS/reports etc. to the Bank as and when required.
- l) **Working days:** Onsite support should provide onsite support during all days when the centralised processing centre is working. Further, if any L3 support is required on those days .Bidder should make L3 support available.

31. The bidder should provide platform for centralized incident management / ticketing solution.

32. Training:

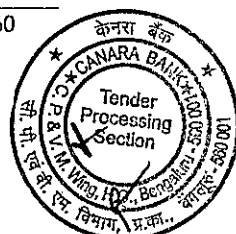
- i. Admin Users of the application to be trained at the Bank's premises
- ii. User's Training - to be conducted at the Bank's Premises
- iii. The training should cover the following areas:
 - a. Functional, Customization development, parameterization, Impact analysis, System and application administration, Log analysis and monitoring and troubleshooting processes, scanning of documents, Preparation of Job card.
 - b. The thorough training for section in charge / Second lines /overseeing executives must be conducted for minimum 2 weeks and as and when required.
 - c. Any up gradations / modifications in the application should be educated to Bank users through appropriate training without any additional cost to Bank.

33. The application processing involving data entry and authorization (i.e., Authorization levels involving Maker Checker concept at various stages/levels) at branch and customer level

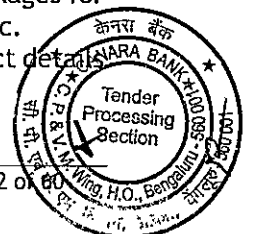
34. The application processing involves compliance check and accounting entry (by assigned user roles) at centralised processing centre level.

35. The application must provide a centralized module for managing user profiles and role assignments for admins, super admins, branches, centralized cells, customers, and auditors (internal and external) with following capabilities: -

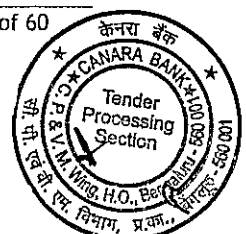
- a. The application must implement Role based access control, allowing permissions for various roles (admin, super admin, customers etc.), ensuring access is limited based on roles and responsibilities
- b. Admins must configure login access and levels of approval (e.g., Maker, Checker, Approver)
- c. The application must integrate biometric authentication mechanisms for secure access user access to the system.
- d. The application must integrate with Bank's HRM API for user management.



- e. The application must ensure multi-factor authentication is available to enhance security, requiring users to verify their identity using multiple methods such as password, OTP etc.
 - f. Super admins should be able to configure multi-level approval workflows, with the ability to push contracts back to any previous level with remarks.
 - g. Admins must provide customers with configurable access to various functions (input, authorize, delete, view, etc.) and allow them to define multiple makers and checkers for different products like LC, Bills, Forwards, and Remittances.
 - h. The system should integrate with Internet Banking or offer a dedicated web-based application for customer access via the internet.
 - i. Admins must be able to add, delete, or modify fields, statuses, transaction flows, and create new forms, with configurable workflows for specific modules or customers, including compliance levels.
 - j. The system must allow configuration of trade and non-trade products, with validation rules and exceptions based on product type, transaction amount, and event criteria.
 - k. Admins should assign role-based access controls, mapped to the HRMS package for role creation and modification based on branch, product, transaction type, or region.
 - l. Admins must manage product allocation to branches, configure product-specific routing rules, and map new branches to regions or zones.
 - m. The system must support dynamic report generation, including daily, monthly, and exception reports, customizable by user, branch, product, region, or transaction type.
 - n. Admins should create, disable, enable, or terminate users and assign sub-admin privileges, while configuring operational modes and privileges for different users.
 - o. Admins should manage document indexing, assign document names and types, and configure internal/external rejection reasons, hold reasons, and pop-up messages for errors or overrides.
 - p. The system must enforce transaction thresholds and notify customers about changes in beneficiary details.
36. The application should have API with the Bank's CBS, Bank's existing other internal applications and be capable of integrating with Bank's any future critical internal applications. This internal API integration should be capable for:
- a. To fetch select details of all customers from CBS including any change of customer data for ex., name, address, contact details, KYC change of branch in CBS, customer MIS should be dynamically synchronized. (i. e) Customer 360
 - b. To fetch select details of all accounts customer id wise for ex., account type, product code, product name, product currency, account status, account balance etc. from CBS and should be dynamically synchronized. (i.e) Accounts 360, Advances 360s
 - c. To fetch details of all limits and liabilities customer id wise for ex., account type, product code, product name, product currency, account status, limit and liability, Account MIS as on date etc. from CBS and should be dynamically synchronized.
 - d. To fetch details of users to define roles and access in the application from bank HRMS application.
 - e. The application should support API integration for Alternate Channels Digital Banking Facilities of the Bank sEx: Mobile Banking, Internet Banking, API Banking, Chat bot, WhatsApp Bankings or any other application in bank etc.
 - f. The application should support API integration with other internal software packages for ex., XMM package, RETAD package, TRACCS, Dealer Pad, AML, KYC screening etc.
 - g. The application should have a provision to link deal rate details / forward contract details for forex transactions and the same is to be extended for customer portal.

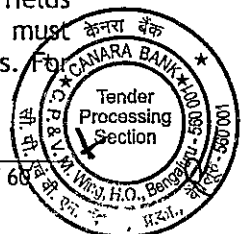


- h. The application should have a facility to verify the Signature for the respective transactions with integration with CBS-FCR at all levels (Branch/CENTRALIZED PROCESSING CENTRE).
37. The application should have interfaces with The Bank CBS to exchange required data in bidirectional.
38. The architecture should be API driven that allows seamless integration with external systems including future versions or additional modules. Application should have the capability to integrate with any other application that may be provided by any third party agencies / government authorities. Application should have the capability to integrate with any other application that may be provided by the third party agencies / government authorities.
- a. The application should support API integration with external software packages / applications/Websites of Regulators/Government bodies for ex., RBI, DGFT, Customs ICEGATE, Express Cargo Clearance System (ECCS), IDBRT, NESL, ECGC, Income Tax, GST, UDIN ICAIss etc.
- b. The application should support API integration with other external software packages/applications/websites for ex., standard model API of ICC & SWIFT, Inco Terms API of ICC, IBAN, SWIFT, Sanction Lists- OFAC, Trade Assets, Vessel Tracker, Trade Finance APIs, Credit Information Companies etc.
- c. The application should be future proof to have capability for API integration with SWIFT and its future releases in specific with "Funds / FIN-plus", MX 2024 release of SWIFT etc.
39. The application should support API integration or independently support generation of Text documents or PDFs by consolidating data outputs from various functionalities. In addition to generation, archiving of the same for anytime future access. The application must have capability to digitally sign the generated documents.
- a. For instance, generation of draft BG, draft LC which shall be mutually approved by all the stake holders. Ex.: Branch user, customer/s and CENTRALIZED PROCESSING CENTRE user.
- b. For instance, generation of debit advice, credit advice, and delivery reports etc.
40. The application should include user interface that features cascading menus, forms, input text fields, selection controls for ex., radio buttons, checkboxes, drop down menus, list boxes, submit buttons, action buttons, file upload fields, drag and drop Areas, calendar inputs, date and time picker, toggles, switches, pop ups, tool tips, validation feedback viz. prompt messages, error messages etc. These cascading menus should provide a hierarchical structure that allows users to navigate through multiple levels of options, ensuring ease of access to various functionalities and select the type of product / functionality / transaction.
41. The application user interface design for customer to be highly user friendly, focusing on ease of use, accessibility, intuitive interaction and navigation. The application must have capability to obtain user feedback and mechanism to address the same.
42. The application should have screen to display summary of transactions module wise as a list with required columns along with facility to search, sort, filter and export to Excel file. The list should have "drill down" feature to allow users to navigate from summary level of data up to detailed view of specific transaction and fall back seamlessly.
43. The application should include functionality to mark or flag rows/transactions for further attention or processing
44. The software application must feature an interactive tables or data grid or spreadsheet-like interface for certain modules, which dynamically displays data loaded from the underlying

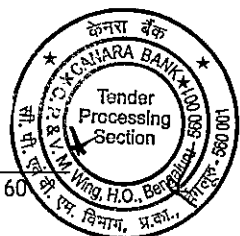


database. The tables shall be non-editable in general and editable in required stages. The tables should support the following functionalities:

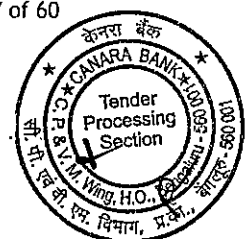
- a. The tables must retrieve and display data from the database in real-time or near-real-time, ensuring that the displayed data is always current and accurate.
 - b. The tables should be mergeable to create new table with joint columns
 - c. The tables should support pagination or infinite scrolling for handling large datasets, ensuring smooth user experience without performance degradation.
 - d. The Users must be able to sort data by column headers and apply filters to narrow down the displayed data based on specific criteria.
 - e. The tables should allow inline editing of data cells, with changes automatically saved back to the database upon user confirmation by button clicks.
 - f. The Users should have the option to export the data from the grid to common formats for ex., Excel, CSV, or PDF.
 - g. Data displayed in the tables must respect user access controls, ensuring that sensitive information is only visible to authorized users.
 - h. On click of actionable events for ex., save, export to database the table data should be exported to different databases which shall be accessible for data dependent modules.
45. The application should provide a secure file upload facility supporting various file types, including documents (ex: PDF, docx), images (ex: jpg, png), excel files. There should be a system to enforce a configurable maximum file size limit and allow multiple file uploads with progress indicators.
46. The application should provide options to centralized processing center users to both download as well as view within the application, the attachments uploaded by front end users (i.e. Branch user, Customer).
47. Various features for the manipulation of images like reverse image, zoom, drag zoom, black and white views, etc., shall be provided.
48. The application shall be used for both on-line and offline image capture in a distributed and centralized platform
49. Depending upon the selection of the transaction/product, the application shall list the required relevant documents and there should be option for admin/super admin to configure the list of requirement of documents for each type of transactions/products/functionalities with mandatory and optional fields. Unless & until all mandatory documents as per the requirement list are uploaded by the Maker, the application shall not allow the data/images to be transmitted to the Checker.
50. There should be predefined templates of various FOREX/INLAND application forms as per the Bank format provided in this application and could be added/modified/deleted at any point in time. The application should also have a facility to create a template at the product level and event level for email and transaction with placeholders for value. The application must be able to auto generate and provide template to customer based on repetitive transactions in customer portal.
51. The application should have limited screens of work flow with important / critical fields related to the required modules and the same should flow to CBS. The application must enable select operations by respective branch on their customer submitted contracts. ex., View, forward, pushback etc.



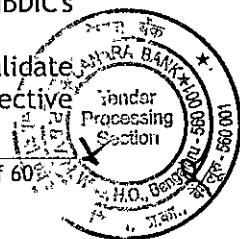
63. The application must facilitate API integration with mail client or possess the capability to autonomously dispatch automated emails from multiple mailboxes triggered by various events/actions from application modules. The automated Emails should incorporate both predefined templates and dynamic data generated by various modules. The application must facilitate API integration with mail client to enable the user to view mail/reply mail/view attachment within the application itself. The application must also possess the capability to auto read emails from select mailboxes, based on predefined text, classify the data read and push down to select modules / functionalities.
64. The application should have a Statutory Compliance module to incorporate compliance check for various statutory norms for ex., RBI, FEMA, AML, Customs, GST, Income Tax, DGFT etc; The module should have "Dynamic Rule Engine" component that allows definition, modification, execution and management of business/compliance rules without need for changes in underlying codebase. It should be designed to be highly flexible and adaptable to frequent changes, especially in regulatory environments. There should be a user interface for defining and managing rules, so as to enable admin user to create or update rules as and when required by the Bank.
65. The application must have various data validation modules with integration to statutory bodies, for ex., PAN validation from Income tax dept., GST no validation from GST dept., UDIN validation from ICAI, IE Code & HSN code validation from DGFT, etc.
66. The application should have repository module for maintenance of various repositories for ex., sanction repository, eTransactionSlip repository, tele quote repository, better rates repository, etc. maintained typically as a table/list, saved unique parameter wise. Each row should be retrievable from any clickable event from any module and displayed in a modal dialog or embedded window with all columns displayed in a predefined format or data flow.
- For instance, Sanction Repository shall contain details of all sanctions of various limits customer wise along with scanned copies of sanction memorandum of various FB & NFB limits with history in chronological order and when a user clicks a button to check sanction of a facility, the particular row to be displayed in a modal dialog.
67. The application should provide super admin with rights to define a template, table and add, delete, maintain list of referential data. For instances: -
- a. Data table(s) containing exhaustive list of countries and with various column level flags for ex., FATF_blacklisted, FATF_greylisted, OFAC_sanctioned, Restricted etc.
 - b. Data table(s) containing exhaustive list of RBI purpose codes for outward remittance
 - c. Data table(s) containing list of details for ex., states and their stamp duty
 - d. Data table(s) containing exhaustive list of charges, commission product wise, transaction wise etc.
 - e. Data table(s) of details of holidays at zone wise, currency wise and year wise
 - f. Data table(s) of zone wise and currency wise Nostro maintenance for every currency and also to maintain Nostro at product level
 - g. Data table(s) for maintenance of state wise maintenance of stamp amount with automated accounting entries both for debiting and crediting parts with proper reconciliation mechanism. (For eBG).
68. The application should have comprehensive exception/error handling and should able to see all exceptions, give overrides and reasons for rejection.
69. Export data Module: -



- a. The application should have Export data module with functionality to export any combination of data from the application to CBS and data flow to be consistent, seamless and well integrated with the fields of CBSs
 - b. The application must support for multiple customizable data export formats for ex., JSON, XML, CSV and etc. to ensure compatibility with the target systems with efficient data mapping & transformation. There should be implementation of a data mapping layer to map internal data structures to the required format of the CBS which includes transformation logic to convert data types, normalize fields, and aggregate data as needed.
 - c. There shall be both batch processing (scheduled exports) and real-time data export (event-driven or on-demand) depending on the business requirements with data Integrity and Validation.
 - d. The application shall ensure that data is encrypted using industry-standard encryption protocols and ensures that the data export module complies with comprehensive logging for all data export operations, including success and failure.
 - e. The data export module should handle large volumes of data to avoid performance bottle necks, with implementation of load balancing to ensure that the data export operations are distributed evenly across resources, improving reliability and performance.
 - f. The data export module should be developed with a modular architecture to easily accommodate future enhancements, for ex., support for additional data export formats or integration with new applications.
70. The Application should integrate with the Bank's existing SMS/Whatsapp/email alerts facility. Application should have a provision to send notifications by auto/manual mode and create notifications at the Bank level at the customer portal side and the Bank side workflow at the event of each application lifecycle events.
71. The application should have an audit trail for all levels of transactions including the customer portal. There should be Audit Trail and Logging feature to capture record of all user activities within the application. This should include actions for ex., logins, data access, document handling, approvals, and modifications, with each entry clearly time stamped and associated with the user who performed the action. The audit data should be exportable in standard formats for reporting and audit purposes. Access to the audit trail should be available only to admins and designated users. Timestamp should be captured for each transaction along with the IP Address of the system of the user.
72. The Application should have a dashboard for Customer, Branch, and Centralized Processing Centre to monitor the transactions providing various data analytics on the operations. The application should provide a Complete Dash Board providing a 360-degree view of applications submitted. i.e., No. of applications submitted, how many are processed within 24 hours, how many are processed within 48 hours, and age-wise TAT. The consolidated data when double-clicked should be able to show the bifurcation Product-wise, Circle-wise, RO-wise, Customer-wise, etc.
73. The application should support API integration or independently support Optical Character Recognition (OCR) for extraction and analysis of text from scanned documents. The application should automate the extraction and analysis of data from trade documents such as invoices, bills of lading, letters of credit etc. reducing manual data entry errors, speeding up processing times with improved accuracy. The Output of OCR must be editable/correctable by users for further processing.



74. The application should have a report module with various customizable reports, module wise, integrating all modules to track key metrics for ex., user performance, TAT, pendency, pushback etc., to gain insight into efficiency, delays, and bottle necks. The report module should be in sync with the dashboard and also in real time. The report module should have capability to generate custom reports as and when required time to time. The report module should be standalone providing reports with specific real time data and comprehensive (T-1) data, yet non-impacting the performance of application core functionalities. The report module also should feature “drill-down” feature to derive from the extensive data set. The reports mentioned in the functional specification of this document are to be provided in addition to the standard reports readily available/configurable in the solution.
75. The application should have Risk Assessment module that evaluates each contract / transaction upon various risk parameters for ex., country risk, currency risk, counterparty risk, nature of transaction etc. and assess a risk scoring, which shall be an integral crucial data of the contract/transaction, providing improved compliance, enhanced decision making etc. The module should analyze historical data and current trends to predict risks associated with trade transactions such as defaults or fraud and prompt warnings to enable informed decision making by User. The application should have business intelligence with interactive dashboard and data analytics modules with capability for descriptive and predictive data analytics capability to provide business insights, trend analysis, fraud detection, pattern recognition etc.
76. The application should have capability to have inbuilt or integrate AI tools for Fraud detection and prevention by way of pattern recognition. That is, the application should detect unusual patterns in transactions that might indicate fraud. For ex., Identification of duplicate invoices, suspicious changes in transaction amounts, abnormal transaction frequencies etc. The application should be able to analyze behavior of entities involved in trade transactions to identify anomalies that could indicate fraudulent activity.
77. The application should be capable of handling digital signed documents for ex., e Bill of Lading, e-Way Bill etc. in general and eBankGuarantee (eBG) specifically, ensuring interoperability, security, compliance, and efficiency. The system must support industry-standard digital signatures to ensure the authenticity & integrity of digitally signed documents.
78. The application should have the capability to leverage block chain and smart contracts for managing trade finance contracts (For example)s e-Bank Guarantees (e-BGs). This includes using a decentralized and immutable ledger to ensure secure, transparent, and efficient handling of e-BGs. The application should record all transactions—issuance, amendments, and invocation—in a tamper-proof manner, accessible in real time by all stakeholders. Smart contracts should be integrated to automate the execution of e-BGs based on predefined conditions, reducing manual processing, minimizing errors, and ensuring swift fulfillment of obligations.
79. The application must offer a comprehensive API suite for corporate customers, ensuring seamless integration with their ERP systems. It should support secure data exchange, real-time notifications, and easy implementation through well-documented APIs. The suite must include version control and testing environments to maintain reliability and accommodate future business needs.
80. The application must be able to integrate seamlessly with the upcoming Indian Banks' Digital Infrastructure Company (IBDIC) application developed by the 18-bank consortium led by the Indian Banks' Association (IBA). It must also maintain alignment with regulatory requirements to facilitate compliance and ensure seamless integration with IBDIC's digital infrastructure. These enhancements are to ensure operational readiness for collaboration with IBDIC's platforms, supporting the digital transformation objectives of the banking sector.
81. The proposed solution must automate invoice matching with supporting documents, validate compliance with trade finance policies, and detect duplicates or discrepancies for corrective



The proposed solution must include a secure customer portal for invoice submission and status tracking, while ensuring document security through encryption, role-based access, and a complete audit trail.

82. The bidder has to **ensure** that application should be scalable to accommodate future change request, API integration, additional modules, data etc.
83. The Proposed solution should integrate with the Bank's API platform.
84. The Proposed solution should have capability of interacting/integrating/maintaining Software Bill of Materials (SBOM). It is a list of all the components, libraries, and modules that make up a software, providing transparency into its composition. Software composition is important to comprehend as it grows more sophisticated and depends on more external components. In cybersecurity, safeguarding software against cyberattacks requires an awareness of the dependencies and components utilized in its construction. An SBOM is therefore a crucial instrument in contemporary cybersecurity procedures.

An SBOM is vital for maintaining software security. It helps organizations understand what their software is made of, manage potential risks, respond to security issues, and comply with regulations.

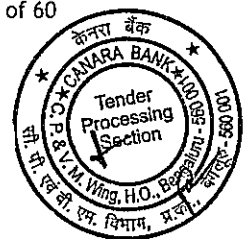
85. EDPMS and IDPMS mapping with banks TRACCS package

The Digital solution to help the customer to report Import and Export transaction to bank and subsequent reporting to RBI digitally, accurately, and unambiguously.

- Digital Platform for customer for trade compliance integrated with TRRACS.
- Availability of RBI Export and Import Dataset to Customer Online.
- Availability of Bank Remittance dataset for the customer Online.
- Dashboard.
- Export and Import Bill Outstanding's.
- Export and Import Remittance Outstanding's.
- Export and Import Bill Aging.
- Export and Import Remittance Aging.
- Real time Integration with Bank Workflow / Trade Processing System.
- Real time Integration with TRRACS.
- Provision for Customer to raise service request against all EDPMS / IDPMS Processes.
- Provision for customer to submit Import Payment request against advance /open account / warehouse transactions.
- Maker / Checker provision for all service request.
- Provision for customer to download MIS reports online.
- AD Transfer Request.

85.1. EDPMS Process Mapping in proposed solution application with TRACCS

<u>SL</u>	<u>Processes in RBI EDPMS</u>	<u>Process available in TRACCS/CBS</u>	<u>Possible System Integration</u>
<u>1</u>	<u>AD Transfer Request</u>	<u>Yes</u>	<u>TRRACS</u>
<u>2</u>	<u>Bill Lodgement</u>	<u>Yes</u>	<u>Core Bank System</u>
<u>3</u>	<u>Bill Lodgement & Realization</u>	<u>Yes</u>	<u>Core Bank System</u>



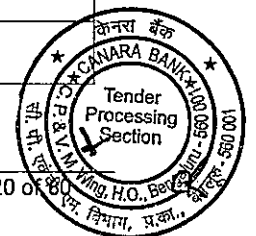
4	<u>Bill Realization</u>	<u>Yes</u>	<u>Core Bank System</u>
5	<u>Bill Extension</u>	<u>Yes</u>	<u>TRRACS</u>
6	<u>Bill Adjustment / Closure</u>	<u>Yes</u>	<u>TRRACS</u>
7	<u>eFIRC Against Inward Remittance</u>	<u>Yes</u>	<u>TRRACS</u>
8	<u>Inward Remittance Adjustment / Closure</u>	<u>Yes</u>	<u>TRRACS</u>
9	<u>Inward Remittance Adjustment / Closure</u>	<u>Yes</u>	<u>TRRACS</u>
10	<u>eBRC Report</u>	<u>Yes</u>	<u>NA</u>

85.2. Exports Reports required from proposed solution

<u>SL No</u>	<u>Report Name</u>	<u>Purpose</u>
1	<u>Export Bill Outstanding Report</u>	<u>User can view the shipping bill that has been outstanding</u>
2	<u>Service Request Report</u>	<u>User can view the status of the service request</u>
3	<u>eFIRC Issuance Report</u>	<u>User can view the list of eFIRC that has been issued.</u>
4	<u>Lodgement Report</u>	<u>Lodgement details can be viewed</u>
5	<u>Lodge and Realization Report</u>	<u>User can check the IRM/FIRC amount that has been settled against the shipping bill.</u>
6	<u>eBRC Issuance Report</u>	<u>User can view the list of eBRC that has been issued.</u>
7	<u>Inward Remittance outstanding Report</u>	<u>User can check the status of the Outstanding inward Remittance.</u>
8	<u>Realization Report</u>	<u>Realization details can be viewed</u>

85.3. Process Mapping in proposed solution application with TRACCS

<u>Processes in RBI IDPMS</u>	<u>Process available in TRACCS/CBS</u>	<u>End Integration System</u>
<u>Manual BOE Creation</u>	<u>Yes</u>	<u>TRRACS</u>





<u>Payment initiation against Invoice (Open AC/Warehouse/Advance)</u>	<u>Yes</u>	<u>Core Bank System</u>
<u>Other Bank BOE</u>	<u>Yes</u>	<u>TRRACS</u>
<u>BOE Invoice to ORM Settlement</u>	<u>Yes</u>	<u>TRRACS</u>
<u>BOE Extension</u>	<u>Yes</u>	<u>TRRACS</u>
<u>BOE Invoice Adjustment /Closure</u>	<u>Yes</u>	<u>TRRACS</u>
<u>ORM Adjustment /Closure</u>	<u>Yes</u>	<u>TRRACS</u>

85.4. Export Reports required from proposed solution

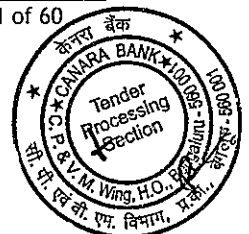
<u>Report Name</u>	<u>Purpose</u>
<u>BOE Settlement Report</u>	<u>User can check the BOE which are settled against Partly Utilized and completed ORM.</u>
<u>Service Request Report Other Bank BOE</u>	<u>User can check the status of the raised Other Bank BOE.</u>
<u>Process Automation Report Invoice to ORM Mapping</u>	<u>User can check the status of the BOE which has been mapped to the ORM.</u>
<u>ORM Outstanding Report</u>	<u>User can check the ORM which is outstanding whose status is either Un-utilized or Part Utilized.</u>

86. Forex related proposal managing and covering GR Waiver and Project Exports.

86.1. module

The application must provide a centralized module for managing the forex related proposals seeking permission from RBI with the following capabilities:

1. Under the centralized module, separate sub modules should be there to handle the following cases:
 - a. RBI permission for forex trade and non-trade transactions
2. To fetch details of all existing customers from CBS including any change of customer data for ex., name, address, contact details, KYC change of branch in CBS, customer MIS should be dynamically synchronized or facility to input the details of the customers manually.
3. Charges to be debited automatically from the account on completion of the transactions.
4. Facility to upload transaction related scanned documents.



5. Tracking/search facility to know the status of activity for any particular transaction. (Status and sub-status should be configurable in the system and the same can be used for any kind of contract/module to track the time taken in each step).
6. Provision should be there to link the previous related transactions.
7. Configurable transaction escalation matrix facility should be available.

Additional module covering the following transaction Types

1. Overseas Direct Investment (ODI)
2. External Commercial Borrowings (ECB)
3. LO/BO/PO (Liaison/Branch/Project Offices)

86.2. Brief Requirements

1. Customer Management
2. UIN/LRN Management
3. Transaction Processing
4. Compliance & Reporting
5. Workflow Management
6. Charge Management
7. Document Management
8. Alert & Notification System

86.3. Customer Management

1. Centralized customer master with unique Customer ID
2. Customer classification (Individual/Corporate)
3. Multiple UIN mapping to single customer
4. Customer group management
5. Provision to capture legacy data
6. Contact management

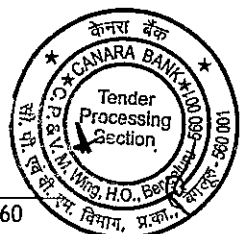
86.4. UIN/LRN Management sub Module

1. UIN/LRN creation and maintenance
2. Multiple transaction types under single UIN/LRN
3. Historical data maintenance
4. Status tracking (Live/Suspended/Closed)
5. Document repository per UIN/LRN
6. Overseas entity details
7. Investment structure details
8. Step-down subsidiary tracking

86.5. Transaction Processing

86.5.1. ODI sub Module

1. Equity investment tracking



2. Loan management
3. Guarantee issuance and monitoring
4. Financial commitment tracking
5. Disinvestment processing
6. APR submission tracking
7. Inward remittance recording

86.5.2. ECB sub Module

1. ECB registration/ Form ECB processing
2. Drawdown management
3. Principal repayment tracking
4. Interest payment scheduling
5. ECB-2 return filing
6. Changes in ECB parameters/ Revised Form ECB processing

86.5.3. LO/BO/PO sub Module

1. Initial permission tracking
2. Extension management
3. Activity monitoring
4. Annual filing management
5. Office closure processing

86.5.4. Compliance & Reporting sub module

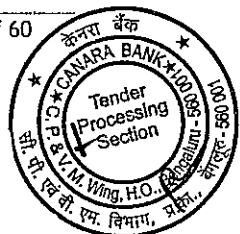
1. Regulatory return generation
2. Compliance calendar
3. Due date tracking
4. Exception reporting
5. MIS reports
6. Audit trails
7. Regulatory submission tracking
8. Investigation case management

86.5.5. Workflow Management sub module

1. Role-based access control
2. Maker-checker framework
3. Multi-level approval workflow
4. Task assignment and tracking
5. Document routing
6. Exception handling
7. Escalation matrix

86.5.6. Charge Management sub module

1. Fee configuration



केनरा बैंक  Canara Bank

2. Charge calculation
3. Invoice generation
4. Payment tracking
5. Revenue recognition
6. Pending fee alerts
7. Integration with accounting system

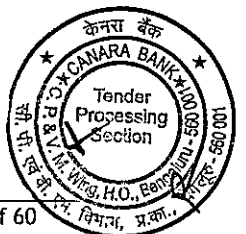
We comply with the above Scope of Work; Non-compliance to any of the scope of work will lead to disqualification in Technical proposal.

Date:

Signature with seal

Name:

Designation:



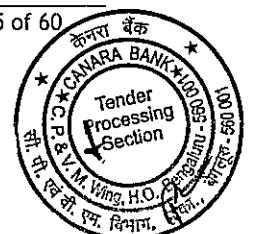
Amended Annexure-8 (A)
Sizing of Hardware including Software/OS for UAT, DC & DRC

(to be submitted on the letter head of the company/firm with authorized signatory seal and sign)

Quoted Hardware/Software/OS details for proposed Document Management Solution for Global Trade Processing Centre in UAT, DC & DRC Locations:

- 1) The bidder shall be responsible for Supply, Installation, Integration, Implementation and Go-Live of the proposed Document Management Solution for Global Trade Processing Centre including the necessary Licenses, Hardware, Storage, Software, Middleware, Database, Operating System, Warranty support. Warranty Support shall be available for the period of 3 years and AMC Support for the period of 2 years thereafter.
- 2) The bidders are required to quote for the entire solution including any Licenses, Hardware, Software, Middleware, Database, Operating System, Warranty support, etc. as may be required to fulfil the entire scope and requirements of the GeM bid.
- 3) The details of all such Licenses, Hardware, Software, Middleware, Database, Operating System, etc. as quoted by the bidder should be provided in the below format along with the Technical Bid.

Sl. No.	Components (Hardware/ Software) (specify the list of items)	Qty	Item Description With Specification Details	OEM of the Product	Model/ Version Name	Date of Release of Product	Date of End of Sale	End of Life (EOL) detail of the offered Product	End of Support (EoS) detail of the offered Product
1.	Hardware/ Appliance including OS for DC		App Server						
			Web Server						
			Data base Server						
			Any other (add more rows of required)						
			<u>Necessary SSL Certificate for all Applications</u>						
2.	Hardware/ Appliance including OS for DRC		App Server						
			Web Server						
			Data base Server						
			Any other (add more rows of required)						
			<u>Necessary SSL Certificate for all Applications</u>						
3.	Hardware/ Appliance including OS for UAT		App Server						
			Web Server						



		Data base Server								
		Any other (add more rows of required)								
		<u>Necessary SSL Certificate for all Applications</u>								
4.	Database Licenses									
5.	Any other Software/ Licenses									
6.	Any other Items									

DC (Should be in onsite) & DRC Site (High Availability and in Sync DC Setup) - Bidder should suggest the architecture in consultation with solution architect along with justifications and should provide reasonable hardware components as per the requirements. DRC should be the replica of the DC site.

In case proposed database is Oracle, then Bank will provide the License. If Database is other than Oracle, Licenses to be provided by Bidder. Bidder has to quote the same in the Bill of Material.

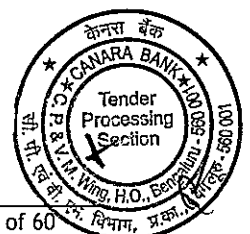
Note: At any point of time during the contract period, the resource utilization like CPU, Memory, Database etc. should not exceed 60 % of the total capacity.

Date:

Signature with seal

Name:

Designation:



Amended Annexure-10
Technical Evaluation Criteria

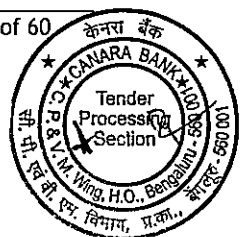
(Should be submitted on Company's letter head with company seal and signature of the authorized person)

SUB: RFP for Selection of Service Provider for Supply, Installation, Implementation, Integration, Customization and Maintenance of Document Management Solution for Global Trade Processing Centre for a period of five years in Canara Bank

Ref: GEM/2025/B/5781717 dated 04/01/2025.

Bank will evaluate the technical proposals of all eligible Bidders based on the documents submitted for the below mentioned criteria:

Sl. No.	Particulars	Scoring methodology	Max Marks	Documents to be submitted For award of mark
1.	<u>The proposed solution should have been implemented/maintaining in any Scheduled Commercial Bank in last Five years as on the date of submission of bid .</u>	No. of Organisations: ≥ 4 organizations: 10 marks ≥ 2 organisations & ≤ 3 organisations: 7 marks 1 organization: 5 marks	10	<u>The bidder/OEM</u> has to provide relevant purchase order/work order / engagement letter & signoff along with satisfactory project completion certificate/ Reference letter from the Concerned Organization / <u>Email reference from the client detailing the services along with Name, Designation, Contact details.</u>
2.	The Bidder/OEM should have implemented/ maintaining Trade Financing Solution in at least one Scheduled Commercial Banks in India having more than <u>1000 branches during last five years as on the date of submission of bid</u>	No. of Branches: <u>≥ 2000 Branches: 10 marks</u> <u>≥ 1000 Branches & < 2000 Branches: 5 marks</u>	10	The bidder/OEM has to provide relevant purchase order/work order / engagement letter & signoff along with satisfactory project completion certificate/ Reference letter from the Concerned Organization clearly mentioning about the bank branches/ <u>Email reference from the client detailing the services along with Name, Designation, Contact details.</u>
3.	The Bidder/OEM must have successfully implemented project of Trade Financing solution in Scheduled Commercial Banks in India during last 3 years from the date of submission of bid.	<u>No. of years:</u> <u>>5 years: 10 marks</u> <u>> 3 years & ≤ 5 years:7 marks</u> <u>up to 3 years: 5 marks</u>	10	The bidder/OEM has to provide relevant purchase order/work order / engagement letter & signoff along with satisfactory project completion certificate/ Reference letter from the Concerned Organization/ <u>Email reference from the client</u>





				be binding on the bidders. It is mandatory for Bidders to have all functionalities listed. Any non-compliance may lead to bidder's disqualification at the sole discretion of Bank.
7.	Bidder's Presentation/ Demonstration	Points will be assigned by an internal committee as per Table P-1	25	Presentation to be conducted as per the schedule provided by Bank.
Total Maximum Marks			100	

Note: The bidder should score minimum 70% of marks out of 100 marks for qualifying under Technical Evaluation. The bidders qualified under Technical Evaluation will be eligible for commercial opening.

Presentation of proposal:

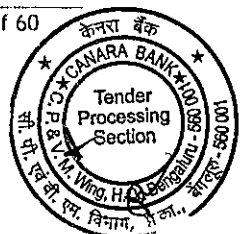
Canara Bank will schedule the presentations and intimate the time and locations to the bidders. Failure of a bidder to complete a scheduled presentation may result in the rejection of that Bidder's proposal.

Table P-1

Sl. No.	Presentation Agenda	Maximum Marks
1.	Work plan and methodology covering complete scope of work	7
2.	Best IT architecture with latest technology, Approach and Methodology	7
3.	Solution's capabilities	5
4.	Compliance, Security & Risk Management	3
5.	Future Scalability	3
	Maximum Marks for Presentation	25

Terms & Conditions

- Bidder to note that all features must be available for demonstration during Presentation/ 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. It is mandatory for Bidders to have all functionalities listed. Any non-compliance may lead to bidder's disqualification.
- Bank reserves the right to conduct interviews of the proposed team members.
- In case of absence of the allotted resource, the standby should perform the job of the absentee.
- Bank may reject such manpower if bank is not satisfied with his/her performance.



Annexure-17
Bill of Material

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

SUB: RFP for Selection of Service Provider for Supply, Installation, Implementation, Integration, Customization and Maintenance of Document Management Solution for Global Trade Processing Centre for a period of five years in Canara Bank

Ref: GEM/2025/B/5781717 dated 04/01/2025

Notes

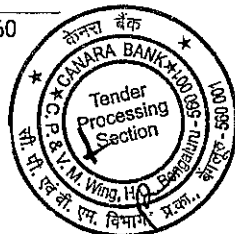
1. These details should be on the letterhead of Bidder and each & every page should be signed by an Authorized Signatory with Name and Seal of the Company.
2. Please be guided by RFP terms, subsequent amendments and replies to pre-bid queries (if any) while quoting.
3. Do not change the structure of the format nor add any extra items.
4. No counter condition/assumption in response to commercial bid will be accepted. Bank has a right to reject such bid.

Table - A

Cost of Hardware & other Items (Including OS & Licenses) for implementation of Document Management Solution for Global Trade Processing Centre

[Amount in Rupees]

Sl. No	Requirement Details	Unit Price with Three years Comprehensive onsite warranty and support (Excl. of Tax)	Qty	Total Cost with Three Year Comprehensive Onsite Warranty and support (Excl. of tax)	Tax for Column c		Total Cost with Three Year Comprehensive Onsite Warranty and support (Incl. of tax)
					% tax	Tax Amt.	
		a	b	c = a*b	d	e	f = c+e
1.	Hardware / Appliance including OS for DC	App Server					
		Web Server					
		Data base Server					
		Any other (add more rows of required)					
		<u>Necessary SSL Certificate for all Applications</u>					
2.	Hardware / Appliance including OS for	App Server					
		Web Server					
		Data base Server					



	DRC	Any other (add more rows of required)						
		<u>Necessary SSL Certificate for all Applications</u>						
3.	Hardware /Appliance including OS for UAT	App Server						
		Web Server						
		Data base Server						
		Any other (add more rows of required)						
		<u>Necessary SSL Certificate for all Applications</u>						
4.	Cost of Database Licenses (In case proposed database is Oracle then, Database cost to be indicated as Zero)							
5.	Any other Software/ Licenses (In case proposed middleware is Oracle Weblogic Enterprise edition then cost to be indicated as Zero)							
6.	Total Cost of Hardware & other Items (Including OS & Licenses) for implementing Document Management Solution for Global Trade Processing Centre(Sum of column F of rows 1,2,3,4 and 5)							

Note: Bidder has to provide the adequate quantity of items in column-b of Table-A as required to cover the entire Scope of Work and Technical Requirements for the entire contract period as mentioned in the RFP document. In future if any additional Hardwares/Softwares are required for the smooth functioning of the solution the same has to be provided by the bidder at no cost to the Bank.

Bidder has to provide the details of all items quoted such as Hardware, Storage, Software, Middleware, Database, Operating System, Licenses, etc. along with its specification details in a separate sheet.

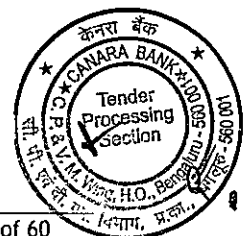


Table - B

Perpetual Enterprise License cost for Document Management Solution for Global Trade Processing Centre with comprehensive onsite Support & Maintenance for 5 Years

[Amount in Indian Rupees]

Sl. No.	Requirement Details	Price details (Excl. of Tax)	Tax for Column a		Total Cost (Incl. of tax)
			Tax %	Tax Amt.	
		a	b	c	d=a+c
1.	Perpetual Enterprise License cost for Document Management Solution for Global Trade Processing Centre with comprehensive onsite Support & Maintenance for 5 Years				
2.	Total Perpetual Enterprise License cost for Document Management Solution for Global Trade Processing Centre with comprehensive onsite Support & Maintenance for 5 Years				

Note: Perpetual Enterprise License with unlimited usage.

Table-C

One-time Implementation Charge

[Amount in Indian Rupees]

Sl. No.	Details	Total Cost (Excl. of tax)	Tax for Column a		Total Cost (Incl. of tax)
			% tax	Tax Amt.	
		a	b	c	d=a+c
1.	One time implementation cost for DC, DRC & UAT infrastructure and Migration				
2.	Total cost for One time implementation at DC, DRC & UAT infrastructure				

Table - D

AMC/ATS cost for items mentioned in Table-A

[Amount in Indian Rupees]

Sl. No.	Description	Post Warranty AMC/ATS Charges year wise					Total AMC/ATS for two Years (Incl. of Tax)
		AMC/ATS Charges (Excl. of tax)		Total AMC /ATS for two Years (Excl. of Tax)	Tax for Column c		
		4 th Year	5 th Year		% tax	Tax Amt.	
		a	b	c=a+b	d	e	
1.	Hardware/ Appliance including OS for DC						
2.	Hardware/ Appliance including OS for DR						
3.	Hardware/ Appliance including OS for UAT						

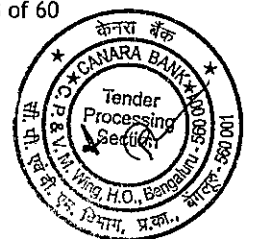


Table-F
Cost for any additional requirements /additional customization/ enhancement
[Amount in Indian Rupees]

Sl. No.	Description	Charges Per Man day (Excl. of Tax)	No. of man days per year#	No. of Year s	Total Cost (Incl. of Tax)	Tax for column d		Total Cost (Incl. of Tax)
						% Tax	Tax amt.	
		a	b	c	d=(a*b*c)	e	f	g=d+f
1.	Cost for any additional requirements/ additional customization/ enhancement		200	5				
Total Cost for any additional requirements /additional customization/ enhancement								

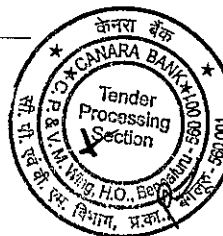
The price quoted by the bidder is fixed for entire contract period and number of man days mentioned above is indicative only. However, the no. of man-days may vary from time to time in total.

Table-G
Total Cost for 5 Years Contract Period
[Amount in Indian Rupees]

Sl. No.	Details	Total Cost (inclusive of taxes)
1.	Total Cost of Hardware & other Items (Including OS & Licenses) for implementing Document Management Solution for Global Trade Processing Centre as per Table-A	
2.	Total Perpetual Enterprise License cost for Document Management Solution for Global Trade Processing Centre with comprehensive onsite Support & Maintenance for 5 Years as per Table-B	
3.	Total cost for One time implementation at DC, DRC & UAT infrastructure as per Table-C	
4.	Total Cost for AMC/ATS for 2 years after the completion of warranty period of 3 years as per Table-D	
5.	Total Cost of Onsite Resources from go-live date as per Table-E	
6.	Total Cost for any additional requirements /additional customization/ enhancement as per Table-F	
7.	Total Cost of Ownership for a period of 5 years [Sum of rows 1,2,3,4,5 and 6]	

Undertaking

- i. Bill of material is submitted on the letter head and is signed by an Authorized Signatory with Name and Seal of the Company.
- ii. We confirm that we have gone through RFP clauses, subsequent amendments and replies to pre-bid queries (if any) and abide by the same.

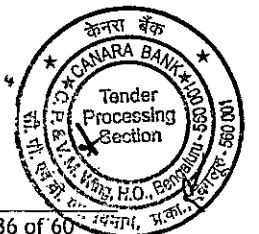


केनरा बैंक  Canara Bank

- iii. We have not changed the structure of the format nor added any extra items. We note that any such alternation will lead to rejection of Bid.
- iv. We agree that no counter condition/assumption in response to commercial bid will be accepted by the Bank. Bank has a right to reject such bid.
- v. We are agreeable to the payment schedule as per "Payment Terms" of the RFP.

Date:
Place:

Signature with seal
Name:
Designation:



- 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
- The Bid Form and the Price Schedule submitted by the Bidder.
 - The Bill of Material.
 - The Technical & Functional Specifications.
 - The Terms and Conditions of the Contract.
 - The Purchaser’s Letter of Intent/Notification of Award.
 - Schedule of Dates, Amounts etc.
 - Pre-Contract Integrity Pact.
 - 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.....

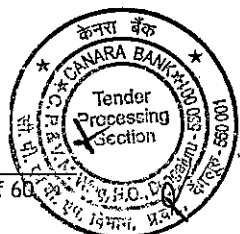
3. TERM OF THE CONTRACT:

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, its 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.

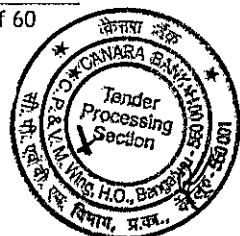
8.2. Notwithstanding the above or any written consent granted by the Bank for subcontracting the services, the Vendor/Service Provider alone shall be responsible for performance of the services under the contract.

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.

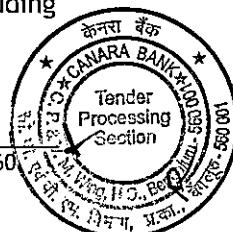
10.2.10. If deductions on account of liquidated Damages exceeds more than 10% of the total contract price.

- 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.

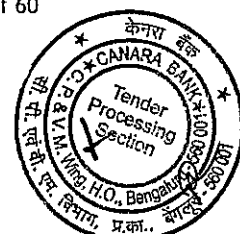
- 10.6. The Bank reserves the right to recover any dues payable by the Vendor/Service Provider from any amount outstanding to the credit of the Vendor/Service Provider, including the pending bills and security deposit, if any, under this contract.



- 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 Tender supplied to the BANK shall not infringe the third party intellectual property rights.



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.

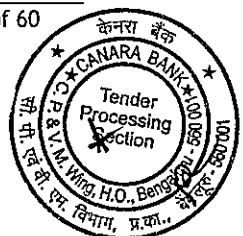
14. INDEMNITY:

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;

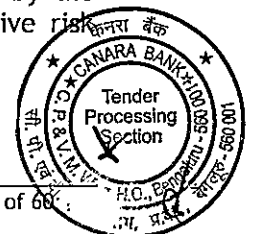
14.1.3. Fines, penalties, or punitive damages levied on Bank resulting from supervisory actions due to breach, default or non-performance of undertakings, warranties, covenants, or obligations by the Vendor/Service Provider



- 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.

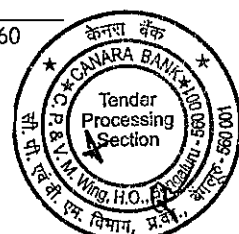
18. CONFIDENTIALITY AND NON-DISCLOSURE:

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.

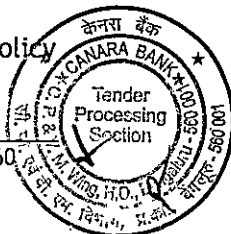
19.4. In such a case, the time for performance shall be extended by a period (s) not less than the duration of such delay. If the duration of delay continues beyond a period of three months, the BANK and VENDOR/ SERVICE PROVIDER shall hold consultations with each other in an endeavour to find a solution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

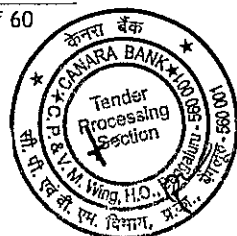
The VENDOR/ SERVICE PROVIDER or subcontractor(s) shall not hire any of the existing/ ex/retired employee of the Bank during the contract period or after the closure/termination of contract even if existing/ ex/retired employee actively seek employment from the VENDOR/ SERVICE PROVIDER or sub-contractor(s). 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



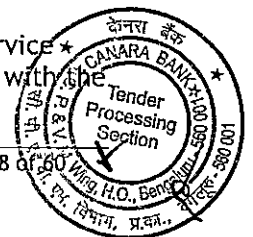
biometric data shall be stored/ collected in the system associated with the vendor, unless allowed under extant statutory guidelines. The vendor shall have a structured process in place for secured removal/disposal/destruction of data and the details of the same shall be provided to the Bank as and when 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 time; 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

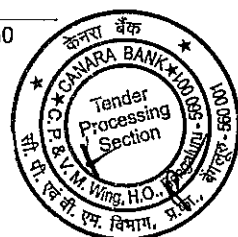
If to VENDOR/ SERVICE PROVIDER:

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.

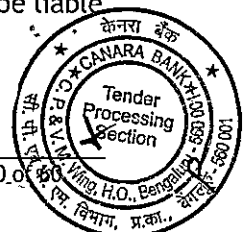
In case of any issue with respect to the execution of the Project, Delivery of Hardware, Services etc., the Bank can escalate the issue as per the escalation matrix.

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	-----	-----	-----	-----	-----	-----

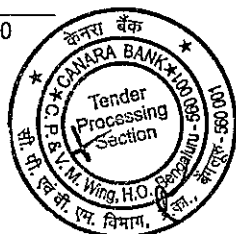
31. GENERAL CONDITIONS TO CONTRACT:

- 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.



केनरा बैंक  Canara Bank

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:

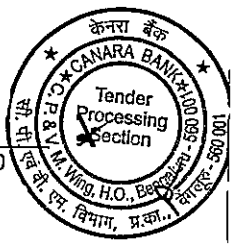
In the presence of:

Signature: 1:
Name:
Designation:

Signature: 1:
Name:
Designation:

Signature: 2:
Name:
Designation:

Signature: 2:
Name:
Designation:



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.

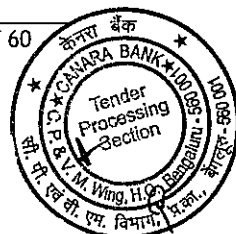
1.1.12. "GDPR" means EU General Data Protection Regulation 2016/679.

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.

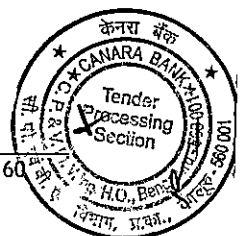
2. PROCESSOR OBLIGATIONS:

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.

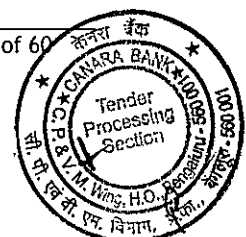
2.3. Sub-Processing:

- 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.

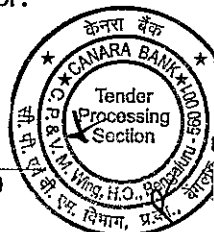
2.7. Deletion or return of Personal Data:

- 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 section 3.7 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.

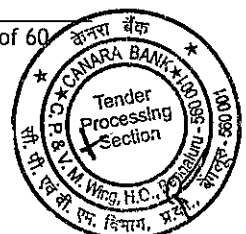
2.12. Agreement Termination:

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:

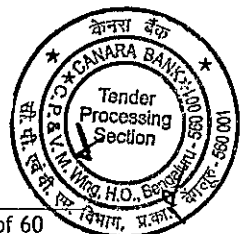
- 3.1. in its use of the services, process the Personal Data in accordance with the requirements of the Data Protection Legislation.
- 3.2. use its reasonable endeavours to promptly notify the Processor if it becomes aware of any breaches or of other irregularities with the requirements of the Data Protection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



Schedule-1

1.1.Services

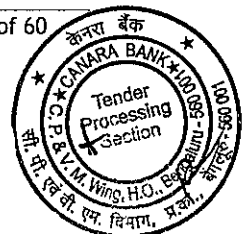
<<Insert a description of the Services provided by the Data Processor (under the Principle Service Agreement, where relevant)>>.



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 27001:2017 and CANARA BANK's Information Security Policy and other related policies/guidelines as appropriate.

