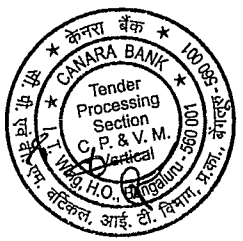
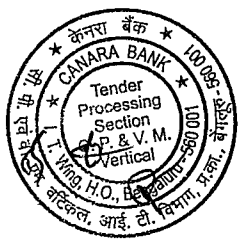
Replies to Pre Bid Queries for GEM/2024/B/4519238 dated 24/01/2024 for Selection of Insurer for Commercial Crime Insurance Policy coverage for the period of one year from 01/04/2024 to 31/03/2025						
Sl. No.	Page No.	Section/ Annexure/ Appendix	RFP Clause	Sub-Clause	Bidder's Query	Bank's Reply
1	General Query				About Insured Company -	Public sector bank
2	General Query				SUBSIDIARIES:	Please refer to our Annaual Report which can be accessed from our website. https://canarabank.com/UploadedFiles/Pdf/01-CB_Annual_Report2022-20231109.pdf
3	General Query				Substantial Shareholders:	Please refer to our Annaual Report which can be accessed from our website. https://canarabank.com/UploadedFiles/Pdf/01-CB_Annual_Report2022-20231109.pdf
4	General Query				Board / Management:	Please refer to our Annaual Report which can be accessed from our website. https://canarabank.com/UploadedFiles/Pdf/01-CB_Annual_Report2022-20231109.pdf
5	General Query				Turnover details -	Please refer to our Annaual Report which can be accessed from our website. https://canarabank.com/UploadedFiles/Pdf/01-CB_Annual_Report2022-20231109.pdf
6	General Query				No. of EMPLOYEES:	84,978* (*as on 31-03-2023)



Replies to Pre Bid Queries for GEM/2024/B/4519238 dated 24/01/2024 for Selection of Insurer for Commercial Crime Insurance Policy coverage for the period of one year from 01/04/2024 to 31/03/2025						
Sl. No.	Page No.	Section/ Annexure/ Appendix	RFP Clause	Sub-Clause	Bidder's Query	Bank's Reply
7		General Query			1. AUDITS - • Do External Auditors audit all operations at least annually? •Inventory Stocks are checked on monthly basis.? •Finance: Are duties segregated so that no individual can control any of the following activities from commencement to completion without referral to others; (a)signing cheques or authorising payments (includingcapital expenditure) above £5,000?Yes ¤No (b)issuing funds transfer instructions? Yes ¤No (c)amending funds transfer procedures?Yes ¤No (d)opening new bank accounts or amending approved signatory details?Yes ¤No (e)investment in and custody of securities and valuables (including blank cheques, travellers cheques, bills of exchange etc.)? Yes ¤No (f)refund of monies or return of goods above £5,000? Yes ¤No (g)disbursement of assets or funds of any Pension Plan?Yes ¤No (h)appointing new suppliers or awarding contracts?Yes ¤No (i)disbursement of loans (including loans to employees) or approving borrowings? Yes ¤No	Canara Bank is a Public Sector Bank and as per the regulatory requirements is subject to strict audit guidelines, The governance mecahnism and audit princliples / framework adopted by the Bank are enlisted as part of the Annual Report . You may refer to the INTERNAL CONTROL AND AUDIT section in the annual report for further details. Please viist the Bank's website for the Annual Report. https://canarabank.com/UploadedFiles/Pdf/01-CB_Annual_Report2022-20231109.pdf

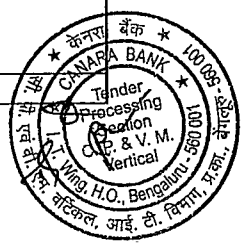
Replies to Pre Bid Queries for GEM/2024/B/4519238 dated 24/01/2024 for Selection of Insurer for Commercial Crime Insurance Policy coverage for the period of one year from 01/04/2024 to 31/03/2025						
Sl. No.	Page No.	Section/ Annexure/ Appendix	RFP Clause	Sub-Clause	Bidder's Query	Bank's Reply
8		General Query			•Computer & Software: oAre unique passwords used to give various levels of entry to the computer depending on the users job functions?/Yes ¤No oAre passwords automatically withdrawn when people leave?/Yes ¤No oAre all amendments to programmes approved independently of the persons making the amendments?/Yes ¤No oAre programmes protected to detect unauthorised changes?/ Yes ¤No oIs your computer system protected by virus detection and repair software?/ Yes ¤No oWhich business activities do you utilise the Internet for? E-Mail / Advertising ¤ Selling Products / Hosting Services for Third Parties ¤ Other- NOT APPLICABLE •Normally How screening of new employees is carried out ? •How Surprise checks/visits are carried out at branches ?	These queries are more relevant to a general business enterprise , however to emphasise the Bank has a stringent Password Protection & Usage Policy and IT Policy which follows the best practice of the Banking Industry and is upgraded at regular intervals as per bsuiness needs and to comply with the Banking Regulator's requirments. Internet is used for all Email communciations, Advertising and Selling of Products. Every Month during the probation period the conduct & performace review of the employee will be submitted to the higher authorities for review.



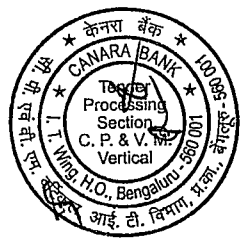
Replies to Pre Bid Queries for GEM/2024/B/4519238 dated 24/01/2024 for Selection of Insurer for Commercial Crime Insurance Policy coverage for the period of one year from 01/04/2024 to 31/03/2025						
Sl. No.	Page No.	Section/ Annexure/ Appendix	RFP Clause	Sub-Clause	Bidder's Query	Bank's Reply
9		General Query			INVENTORY CONTROL - 1.Is there controlled access to all locations? Yes ¤No 2.Are all premises containing stock, money, securities, precious metals etc. connected to an intruder alarm which is connected to a central station or a police station and are such intruder alarms maintained in proper working order?..... Yes ¤No 3.Is an independent physical count of stock, raw materials, work in progress and finished goods undertaken at least quarterly and is this count reconciled against stock records?Yes ¤No 4.Is the transfer of money and securities valued above £10,000 made by a security or professional cash carrying company? Yes ¤No 5.What is the maximum value of money, securities, precious metals and/or jewellery at any one location: (a)during business hours? PLS REFER MONEY AND FIDELITY POLICY (b)outside business hours? PLS REFER MONEY AND FIDELITY POLICY 6.What is the maximum value of stock, work-in-progress and raw materials at any one location? - PLS REFER THE FIRE POLICY	These queries are more relevant to a general business enterprise and please note that the responses will vary from Branch to Branch and maximum value of money, security and precious metals will be difficult to share. Please note that the Bank also has in place a BBB policy and Locker Insurance Policy(as per the mandatory norms) . Details of the same can be taken from the Bank's website (earlier and current tenders). The Bank maintains best in class physical security features at all locations and bracnches as per their internal risk philosphly and as required by the directives of the Banking Regulator.

केनरा बैंक CANARA BANK Tender Processing Section C. P. & V. M. Vertical I. T. Wing, H.O., Bengaluru - 560 001

Replies to Pre Bid Queries for GEM/2024/B/4519238 dated 24/01/2024 for Selection of Insurer for Commercial Crime Insurance Policy coverage for the period of one year from 01/04/2024 to 31/03/2025						
Sl. No.	Page No.	Section/ Annexure/ Appendix	RFP Clause	Sub-Clause	Bidder's Query	Bank's Reply
10		General Query			Third Parties 1.Do you maintain an approved suppliers list?Yes ¤No 2.Are suppliers and service providers: 3.vetted for competency, financial stability and honesty before a.being approved?..... Yes ¤No 4. appointed under written contract? ..... Yes ¤No 5.Are procedures in place to assess the suitability of trustees, fiduciaries, administrators or officers of all of your Pension Plans? Yes ¤No (a)Do you outsource any normal administrative function to a.third party service providers?¤Yes No 6.If "yes", please detail the services and estimated annual contract values. 7.Do you audit outsourcing companies during the term of their contract?Yes ¤No 8.If the outsourcing company operates on your premises are their employees under your daily management control?Yes ¤No	With respect to Third Parties, Supliers and Service Provider,the Bank follows a strict vendor management policy and is guided by the same. The Bank also follows a regular process of vendor audits . Also, the Bank is governed by the RBI's guidleines on IT Outsourcing. The empanellment of all vendors and suppliers is done through a comprehensive procurement process through the GeM portal as per the Finance Mnistry directives. The Bank employs vendors for various business operations and functional requirments. Wherever the outsourcing company operates at the Bank's premises the outsource's employees are manged & supervised by the Bank's officials
11		General Query			BANK ACCOUNT CONTROL - •How Duties are segregated ? •Who has the cheque signing authority ? •All the Promisory notes (BOE, Cheques, Drafts) requires counter signature ? •Instruction Communication to the Bank for Fund Transfer is done by limited set of employees in a prescribed format ?	This question is more attuned towards a regular business eneterprise. The Bank is governed by its internal finace controls and adheres to all structures and principles/directives of the Banking regulator.
12		General Query			SECURITIES •They do not hold or own any kind of negotiable securities in their premises or outside premises ? 6. PRECIOUS METALS •They do not hold or own any kind of precious metals in their premises or outside premise	This question is more attuned towards a regular business eneterprise. The Bank is governed by its internal finance controls and adheres to all structures and principles /directives of the Banking regulator.
13		General Query			7.Claim/ Loss/incident Details of last 5 year	Please refer Annexure II of Replies to Pre-Bid queries



Replies to Pre Bid Queries for GEM/2024/B/4519238 dated 24/01/2024 for Selection of Insurer for Commercial Crime Insurance Policy coverage for the period of one year from 01/04/2024 to 31/03/2025						
Sl. No.	Page No.	Section/ Annexure/ Appendix	RFP Clause	Sub-Clause	Bidder's Query	Bank's Reply
14		General Query			Expiring Policy details	Please note that scope of work and the broad terms and conditions of the policy remain the same for the renewal. New contingencies and exposures proposed for cover on the renewal are API Banking, Digital Lending, AePS Transactions, CBDC. A separate note on the expsoures, security measures, transaction limits for each of these expsoures is provided for your reference.You are requested to refer and review the Scope of Work, and Draft Policy Wordings which form part of the RFP for all details.
15		General Query			Claims paid and outstanding for the last 3 years (in terms of both numbers and amounts)	Please refer Annexure II of Replies to Pre-Bid queries
16		General Query			Preventive measures taken to avoid losses in the last one year	Please refer Preventive Measures - Annexure I of Replies to Pre-Bid queries
17		General Query			New initiative taken to strengthen the system to reduce/mitigate losses	Please refer Preventive Measures - Annexure I of Replies to Pre-Bid queries
18		General Query			ICR Details for past 3 years.	Please refer Annexure II of Replies to Pre-Bid queries
19		General Query			Premium and claim details for past 3 years.	Please refer Annexure II of Replies to Pre-Bid queries
20		General Query			Variations proposed in this renewal.	Please note that scope of work and the broad terms and conditions of the policy remain the same for the renewal. New contingencies and exposures proposed for cover on the renewal are API Banking, Digital Lending, AePS Transactions, CBDC.Please refer Annexure II of Replies to Pre-Bid queries for details on security measures & transaction limits for each of these expsoures.You are requested to refer and review the Scope of Work, and Draft Policy Wordings which form part of the RFP for all details.



Replies to Pre Bid Queries for GEM/2024/B/4519238 dated 24/01/2024 for Selection of Insurer for Commercial Crime Insurance Policy coverage for the period of one year from 01/04/2024 to 31/03/2025						
Sl. No.	Page No.	Section/ Annexure/ Appendix	RFP Clause	Sub-Clause	Bidder's Query	Bank's Reply
21		General Query			Security measures and improvisation measures taken to avoid losses.	Major loss mitigation measures/ improvements put in place for UPI/ IB/MB to prevent frauds- Please refer Preventive Measures - Annexure I of Replies to Pre-Bid queries. Siginificant security measures which are being implemented /are in the process of being implemented too. Introduction of Silent SMS detection & prevention Denying of duplicate registration request Initiation of IVRS call for Payment Gateway transactions
22		General Query			Claims MIS of last 3 years with the details of cause of loss	Please refer Annexure II of Replies to Pre-Bid queries
23		General Query			Please provide the Claims Details of last 3 years	Please refer Annexure II of Replies to Pre-Bid queries
24		General Query			Premium details of last 3 year policies	Please refer Annexure II of Replies to Pre-Bid queries
25		General Query			Whether the terms and conditions given in the RFQ are as per the expiring policy ?	Please note that scope of work and the broad terms and conditions of the policy remain the same for the renewal. New contingencies and exposures proposed for cover on the renewal are API Banking, Digital Lending, AePS Transactions, CBDC.Please refer Annexure II of Replies to Pre-Bid queries for details on security measures & transaction limits for each of these expsoures.You are requested to refer and review the Scope of Work, and Draft Policy Wordings which form part of the RFP for all details.
26		General Query			What are the Major Security measures/improvements taken by the Canara bank recently as a loss mitigation measures , wrt to the losses reporting under the commercial crime policy.	Please refer Annexure I of Replies to Pre-Bid queries: Preventive Measures and Annexure II of Replies to Pre-Bid queriesfor security features of new digital channels
27		General Query			Furnish the last years Claim Experience Details	Please refer Annexure II of Replies to Pre-Bid queries

Date: 14-02-2024
Place: Bengaluru

Deputy General Manager

केनरा बैंक CANARA BANK Tender Processing Section C. P. & D. M. Vertical 1st Wing, H.O., Bengaluru - 560 001

Annexure-I (of Replies to Pre-Bid queries)
Preventive Measures

1. For Online Banking channels transactions, Two Factor authentication mechanism is implemented.

2. Mobile Banking app prevents customers from registering if it detects any desktop sharing apps & Jailbroken/rooted devices on the mobile device.

3. Device and SIM Binding: For registering onto mobile devices, Device and SIM Binding is made mandatory for UPI and Mobile Banking services. Thus, establishing the usage of same combination of SIM and mobile device for carrying out transactions through our mobile applications.

4. Cooling Period for New Users: Restrictions are placed on transactions on the basis of first registration in Mobile Banking (12 hours) & UPI (72 hours).

5. Cooling Period for New Beneficiary: Restrictions are placed on transactions for first 12 hours, on the basis of beneficiary addition in Mobile Banking & Internet Banking.

6. Option to Set Transaction Limits: Internet Banking User can set transaction wise limits and this feature is under implementation in Mobile Banking app.

7. Enterprise Fraud Risk Management (EFRM) rules: Rules based on the pattern of the fraudulent transactions are implemented in our EFRM system for raising alerts and/ or declining transactions altogether.

8. Option to Disable Online Banking Channels: Option to disable Online Banking Channels through different modes by our customers are available i.e Internet Banking, Mobile banking, SMS & Call Centre.

9. Auto-detection of harmful application: Our Mobile Banking application is enabled with auto detection of Remote Control/ Screen Mirroring apps (TeamViewer & AnyDesk) and SMS forwarding applications. In such scenarios, our application will not start and a message will be displayed to the customer mentioning that a harmful application is running in background.

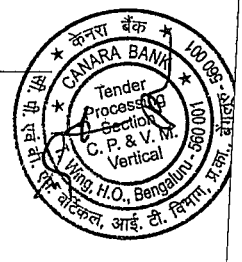
10. Encryption: Strong encryption protocols are used to protect data during transmission.

11. Antivirus Software: Users are encouraged to install and regularly update antivirus software to detect and mitigate malware.

12. User Education: Bank and government agencies conduct awareness campaigns to educate users about online security risks and safe practices.

13. Regulations and Compliance: The Reserve Bank of India (RBI) and other regulatory bodies issue guidelines and regulations to enhance cybersecurity in the financial sector.

14. Fraud Detection Systems: Bank and payment service providers employ sophisticated fraud detection systems to identify and prevent suspicious transactions.



15. Instant Alerts: Users receive alerts for transactions made with their accounts, helping them quickly identify unauthorized activity.

16. EFRM Rules: EFRM is to secure the customers and safeguard the interest of the Bank. For MB, UPI & IB velocity checks are implemented.

केनरा बैंक CANARA BANK Tender Processing Section C. P. & V. M. Vertical I. T. Wing, HO Bengaluru - 560 001

केनरा बैंक Canara Bank

ANNEXURE II (of Replies to Pre-Bid queries):
PREMIUM & Claims Details , New Digital Channels (Security Features and Transaction Limits)

Premium and Claims

Policy Year	Premium
2021-2022	INR 36,000,000 plus GST
2022-2023	INR 21,485,714 plus GST
2023-2024	INR 18,500,000 plus GST

Claims Summary- PY 2021-22, 2022-23, 2023-24.

Year	Outstanding		Settled	
	Count	Loss Estimate	Count	Paid Amount
2021-2022	1	2,20,000	192	20,15,775
2022-2023	77	1,48,93,174	131	29,76,364
2023-2024	605	3,92,74,003	55	17,87,743
Grand Total	**683**	**5,43,87,177**	**378**	**67,79,882**

Note :

Outstanding column reflects the amount claimed by the Insured.

Claims include majorly UPI, Mobile Banking and Internet Banking fraud claims

केनरा बैंक CANARA BANK Tender Processing Section C. P. & V. M. Vertical IT Wing, H.O., Bengaluru - 560 001

केनरा बैंक Canara Bank

NEW DIGITAL Channels (proposed for cover)

Please refer the Scope of Work for understanding of contingencies proposed for cover.

CBDC (Digital Rupee)

- Limits of Transaction in CBDC:

COOLING_PERIOD_ANDRIOD	24 hours
COOLING_PERIOD_IOS	72 hours
CP_LOAD_TOKEN_COUNT	500
PER_DAY_LOAD_TXN_COUNT	10
PER_DAY_TRANSFER_TXN_COUNT	10
NEW_USER_PER_DAY_LOAD_AMOUNT_LIMIT	150000
OLD_USER_PER_DAY_LOAD_AMOUNT_LIMIT	150000
NEW_USER_PER_DAY_TRANSFER_AMOUNT_LIMIT	5000
OLD_USER_PER_DAY_TRANSFER_AMOUNT_LIMIT	150000
OLD_USER_PER_DAY_P2M_TRANSFER_AMOUNT_LIMIT	100000
OLD_USER_PER_DAY_P2P_TRANSFER_AMOUNT_LIMIT	100000
NEW_USER_PER_DAY_P2P_TRANSFER_AMOUNT_LIMIT	5000
NEW_USER_PER_DAY_P2M_TRANSFER_AMOUNT_LIMIT	100000
PER_HOUR_TXN_COUNT	5

Loss Prevention Measure under CBDC: With risk mitigation features, Canara Digital Rupee application adheres for RBI's DPSC guidelines to prevent fraudulent transactions.

Digital Lending:

Limits of Transaction in Digital Lending:

For Digital Lending PAPL (Pre-Approved Personal Loan) product: INR 10 lakh

- Loss Prevention Measure under Digital Lending:

1. SMS/Email OTP based Login
2. Two CICs check
3. Loan will be disbursed to customer own account only where again restrictions are available before debiting the SB amount
4. Online execution of loan documents through NESL based on Aadhar based OTP authentication
5. Repeated SMS alert to applicant including loan disbursement into SB- 4 in numbers in different stages

केनरा बैंक CANARA BANK Tender Processing Section C. P. & IT Vertical IT Wing, H.O., Bengaluru - 560 001

API Banking Solution

- **Limits of Transaction in API Banking Solution:**
  Different transaction limit (Rs. 5 Cr, 8 Cr, 20 Cr and Customised Limit) per day per customer based on customer request and CO recommendations

- **How are these limits spread across / concentrated across various customers - Is there any bifurcation between various customers. If yes, please share customer band wise Limits and number of expected customers within each band.**
  Yes, the limits are assigned based on the customer request and CO recommendations.

- **Number of expected customers to be serviced under API Banking Solution:**
  Appox. 150-200 customers expected to be on-boarded on API Banking by Mar'25.

- **Loss Prevention Measure under API Banking Solution:**

  Following are the security measures being implemented as part of API Banking Platform. It is expected that clients must adhere to the security parameters.

1. **IP Whitelisting:**
   IP whitelisting is a security feature used for limiting and controlling access to trusted users. For Production Environments Bank uses IP whitelisting to create lists of trusted IP addresses or IP ranges from which Client's applications can securely a ccess Bank's API. Client has to share the IP Range in advance.
2. **Client ID and Client Secret:**
   Every API call will be secured by API Key (Client ID and Client Secret). Bank will sha re API key at the time of registering the application. This is for identification and authentication of our client.
3. **Encryption:**
   All communication between Bank and Client has to be encrypted. Encryption will be done using "A128CBC-HS256 algorithm".
4. **Certificate:**
   Client needs to invoke the application over HTTPS protocol only. It is required that the consumer has a valid signed certificate from a registered Certifying author ity. The same has to be shared with the Bank as a pre-requisite at the time of registering the application.
5. Digital Signature:
   All communication between Bank and the Client has to be digitally signed using "RS A- SHA256 Algorithm" and "base-64 encoding".
6. **HTTPS/POST:**
   All API calls should have secure interaction with HTTPS. POST Method to be used for all HTTPS calls. TLS 1.2 or greater version is mandatory for SSL communication.
7. **Input Data/content Validation:**
   All input data will be verified at the Bank end against insertion of any suspicious co de /malicious characters to avoid any insertion attack.

We are taking following steps to mitigate Cyber Security Risk associated with the integration:

- Source Code Audit of the proposed integration.
- VAPT of the Servers by CERT-IN empanelled vendors.
- Integration of system & software with EFRM and SIEM system.
- API Assessment for all relatable APIs.
- Regular updates of Security Patches in software/system.

AePS

AePS is a bank led model which allows online interoperable financial inclusion transaction at PoS (MicroATM) through the Business Correspondent of any bank using the Aadhaar authentication.

Canara Bank has two types of AePS transactions:

ON US: An intra-bank transaction where an Aadhaar-initiated transaction which can be done only in accounts within the same bank and does not necessitate an interbank settlement.

OFF US: An inter-bank transaction is one where there is movement of funds from one bank to another necessitating an interbank settlement. The parties involve in OFF US AePS transactions are acquirer bank, business correspondent and issuer bank.

Business Correspondent is an approved bank agent providing basic banking service using a MicroATM (terminal) to any bank customer wishing to avail their bank BC service.

Limits of Transaction in AePS:

Transaction channl	Transaction type	Per transaction limit	Daily limit		Weekly limit		Monthly limit (Only for AEPS OFFUS issuer)	
			No of transaction per day	Overall limit	No. of transaction	Overall limit	No. of transactions	Over all limit
AEPS (ONUS)	Deposit/ fund transfer/ Withdrawal	10,000	2	20,000	N.A	N.A	N.A	N.A
AEPS (ISSUER)	Deposit/ Fund transfer	10,000			N.A	N.A	N.A	N.A
AEPS (ISSUER)	Withdrawal	10,000		10,000	N.A	15,000	N.A	20,000

AEPS OFFUS Issuer	Mini-statement	N.A	N.A	N.A	N.A	N.A	5	N.A.
AEPS OFFUS Acquirer	Withdrawal/ Deposit/ Funds Transfer	10,000	N.A	N.A	N.A	N.A	N.A	N.A

Appropriate authority can permit the enhancement/ revision in the transaction limits subject to guidelines from NPCI/ GoI. The same shall be implemented after approval from appropriate committee.

- **Loss Prevention Measure under AePS:**

1. Bank has introduced daily, weekly and monthly limit on AePS Off Us transactions (Daily Limit: INR 10,000; Weekly Limit: INR 15,000; Monthly Limit: INR 20,000).
2. Bank has introduced cooling period of 120 minutes between two AePS Off Us transactions.
3. Bank has disabled AePS transactions:
   - for accounts in which the only AePS debit transaction in the past 12 months was reported as fraud
   - For accounts in which there has been no AePS transaction for past 12 months
   - It can be enabled again on customer request after necessary authentication.
4. NPCI is blocking terminal ID of fraudsters through EFRM portal of NPCI.
5. Bank has introduced (FMR-FIR) modality as instructed by NPCI.
   Finger Minutiae Record-Finger Image Record (FMR-FIR) Modality:

   - The FMR-FIR modality is an advanced AI/ML based technology developed by the UIDAI to bolster security measures within the Aadhaar-enabled Payment System.
   - The modality's primary function lies in assessing the liveness of the captured fingerprint.
   - It can differentiate between a genuine 'live' finger and a cloned or fake fingerprint, thereby preventing spoofing attempts.
   - FMR-FIR operates in real-time, providing instant verification results during the authentication process.
   - This technology, specifically designed to enhance Aadhar-enabled Payment System transactions, aims to tackle fraudulent activities, including the misuse of cloned fingerprints as informed by NPCI.
   - UIDAI authentication server is validating the bio metric authentication.

केनरा बैंक CANARA BANK Tender Processing Section C. P. & V. M. Vertical I. T. Wing, H.O., Bengaluru - 560 001