Replies to the Pre-Bid queries for the GeM Bid Ref No.GEM/2022/B/2894320 dated 22/12/2022 for the "Selection of insurer for renewal of cyber risk insurance policy for Canara Bank from 31st March 2023 to 30th March 2024"

S.No.	GeM Bid Clause	Clause / Requirement	Bidder's Query	Bank's Reply
1	NA	NA	Coverage for cost of reissuance of compromised cards post cyber attack Sub limited to INR.100,000,000 - Whether it has not been covered in card policy, if so then is it in excess of that?	This is an exposure that is not under the scope of the Card (Lost card liability) policy.
2	NA	NA	Does the 24/7 SOC extend to all/global operations? Or have differing Security teams depending on where they are in the world?	Yes, the 24/7 SOC extends to all/global operations
3	NA	NA	Insight into how segmented is the business? Do the segment networks geographically, or by division? If one region goes down, does it have the potential to impact another?	Networks are segmented in different geographies in DC & DR locations.
4	NA	NA	US exposure revenue is mentioned as 0.12% for March 2022 and 0.59% for Sept 2022. Can you please share more details on revenue generation from US?	Interest Income (in crores): Mar-22 : 100.83 Sep-22 : 282.82 Other Income: Mar-22 : 0.03 Sep-22 : 1.15 Total: Mar-22 : 100.86 Sep-22 : 283.97 a) Interest income and expenses are linked to the movement in FED rates. #Branch's major portion of operations during the period "April 1, 2022 to Sep. 30, 2022" increased in Money Market operations. #Fed rates increased from 0.4% to 0.9% from May 5, 2022, from 0.9% p.a. to 1.65% p.a. with effect from June 16, 2022, from 1.60% p.a. to 2.40% p.a. with effect from July 28, 2022. #FED rate again increased by 75 bps w.e.f. Sep. 22, 2022 i.e. from 2.40% p.a. to 3.15% p.a. and again increased by 75 bps from Nov. 3, 2022 i.e. from 3.15% p.a. to 3.90% p.a. #The recent FED rate hike was for 50 bps w.e.f. Dec. 15, 2022 i.e. 4.40% p.a. b) Further, the exchange rate movement is one more factor. Exchange rate as on 31-03-2022 was at Rs. 75.7925 and Exchange rate as on 30-09-2022 was at Rs. 81.3450.
5	NA	NA	With reference to the captioned renewal, it is observed from the Tender document, that the GeM portal bidding is proposed on Reverse Auction Method. We would like to express our concern regarding the same. In our opinion, it is not advisable to enter into Reverse Auction bidding for complex and large insurance programs like Cyber Liability. Hence, request you to kindly waive off the requirement of Reverse Auction.	Bidder has to comply with GeM bid terms.
6	NA	NA	IT Business Continuity and Disaster Recovery Policy of Canara Bank	Bank is having Board approved BCP policy.
7	NA	NA	Information Security policy of Canara Bank	Bank is having board approved Information Security policy.
8	NA	NA	Data protection/ Data privacy policy of Canara Bank	Infiormation is submitted as part of the Proposal form.
9	NA	NA	Data system backup & recovery policy of Canara Bank	Bank has Backup policy/Guidelines.
10	NA	NA	Cyber security incident response recovery plan of Canara Bank	Bank is having Cyber Crisis Management plan policy.

D.I.T. Wing, Procurement Group
CANARA BANK
H.O. Bengaluru-560 001

11	NA	NA	Any other plan or Policy with respect to Information Security as designed or developed by the Company	Yes. Bank has Information Security, Cyber Security Policies & Information security guidelines.
12	NA	NA	Along with the above requirements, Please provide the details of the claims History for last 3 years, Brief details on the Claim Status of the claim Claim Amount Preventive measure taken after the claim/Loss Incident by the proposer.	Please refer to the claim note enclosed as Annexure-4.
13	NA	NA	We also request you to kindly wave the Reverse Auction Condition.	Bidder has to comply with GeM bid terms.
14	NA	NA	On going through the tender document we noticed that in para no. 3 'Reverse auction would be conducted '. We request you to please withdraw the said clause, as we being a PSU are not eligible to participate in reverse bidding.	Bidder has to comply with GeM bid terms.
15	NA	NA	Ransomware Supplemental - as per enclosed format	Details furnished in separate enclosure as Annexure-1
16	NA	NA	Details for 12 C - as per enclosed format	Details furnished in separate enclosure as Annexure-2
17	NA	NA	List of subsidiaries to be covered under the policy	Not applicable
18	NA	NA	URL details of all covered entities and subsidiaries	There are approximately 8 domains like canarabank.com, canarabank.in etc. hosting various underlying sub-domains/applications pertaining to the Bank.
19	NA	NA	Queries regarding Log4j vulnerabilities: (Kindly help us with the clarifications on group level) 1. What have you done to identify assets that use Log4j in your environment, especially internet-facing ones? 2. What affected systems have you patched so far, and when did you patch them? 3. How are you handling the potential compromise of those systems? 4. What steps have you taken to block Log4Shell attacks, and what extra monitoring, if any, are you doing?	19.1. All internet facing machines assets have been scanned to check Log4j vulnerabilities. 19.2. The vulnerabilities have been fixed where ever reported. 19.3. No compromise observed on systems. 19.4 Blocking policies are implemented in Firewall, Antivirus and SIEM monitoring also in place.
20	NA	NA	Confirmation that RW supplement represents all regions and all group entities covered by policy. Else, For subsidiaries, request you to kindly confirm if the controls & measures disclosed in RW of Parent's entity will apply to their subsidiaries covered under the policy. If not, then we will require separate RW questionnaire for those entities as well.	RW supplement represents all regions of the Bank.
21	NA	NA	Forensic reports for all ransomware incidents that might have occurred in client's environment in last 18 months, if any.	No incident occurred during the current policy period.
22	NA	NA	Copy of Executive Summary of Penetration testing report, if any.	Not applicable

E.I.T. Wing, Procurement Group ★ CANARA BANK ★ H.O., Bengaluru-560 001

23	NA	NA	1.Whether the networks are connected of the insured and other covered entities (not just by virtue of being connected to the internet). System interconnectivity includes sharing of: 1. Domain 2. Shared Folders 3. Active directory 4. Email systems 5. Security system 6. Network infrastructure 7. ERM or CRM type applications (e.g. SAP, Salesforce, etc.) 8. Common Datacenter / Cloud Tenancy (what about coincidence they use the same company but do not share the same resources - better way to be specific?) 9. Common IT team managing multiple IT environments of group companies (if common, could central team be bridge to incident from insured to none-insured?) 10. End user systems 11. Operational technology 2. Details of the entity and its relationship to the applicant 3. If they are interconnected , what systems/data are exposed 4. What controls are in place to minimise infection/hacking etc. 5. Controls to prevent unauthorised access or use of the applicants computer systems and data.	Not applicable
25	NA	NA	Is system Failure / PCI cover present in expiring policy?	Yes
26	NA	NA	What type of data is stored?	Bank stores Customer PII data and business information related to various Bank's systems and operations.
27	NA	NA	Number of manufacturing locations	Not Applicable
28	NA	NA	Please arrange for following (in case applicable) o PCI DSS certificate. o ISO 27001 certificate.	a.Bank is certified with ISO 27001:2013 certification b.PCI DSS is certified for Card Management System, c.ATM c.Switch is certified with PA-DSS. d.ATM machines are certified with PA-DSS.
29	NA	NA	Do you have Segregation of Network based on Business Function to avoid lateral spread?	Yes
30	NA	NA	Please let us know how a typical BCP testing looks like in terms of Role played by different team and the process	Bank is conducting regular DR drills to ensure robustness of BCP readiness as per Bank's BCP policy.
31	NA	NA	Please let us know how do you arrive at your RTO and RPO	RTO and RPO are estimated considering Business Impact Analysis and Business continuity reuirements and Technology related controls in place to achieve the same.
32	NA	NA	Do you test security functionality during the development lifecycle of information systems incl. IT security updates? If the response is no. request you to kindly share some more details on this aspect?	Yes

D.G.M, Wing, Procurement Group
CANARA BANK
H.O., Bengaluru-560001

33	NA	NA	List of entities and their description that would get covered. We would need to understand the current structure of the IT-Information security team in terms of Roles, function and reporting and Strength (no of people)	No subsidiaries are covered. Information Security functions include: 1. 24*7 monitoring of following security solutions implemented in SOC - SIEM, DLP, NBA, Anti-DDoS, Deception, PIM 2. Incident response and management 3. Quarterly internal VA 4. Annual external VAPT by Cert-in empaneled vendor 5. Red Team 6. DAST 7. Threat Hunding 8. Quarterly Table Top Exercise & Drill 9. Quarterly Phishing Simulation Exercise 10. Cyber Security Awareness 11. Action on Threat Intel Feeds received from CSITE, Cert-In, NCIIPC, IB-Cart, & RSA Feeds 12. Regulatory Compliance Team size of 22 members (Bank & Vendor) consisting of SOC manager, analysts and incident handlers. Team is highly skilled with experience & certifications. • Level 1 (L1) SOC Analyst - 24x7 security monitoring team that reviews and performs initial investigation into security alerts. • Level 2 (L2) Incident Handler - Perform incident investigation and response for frequently occurring or more common security events. • Level 3 (L3) SOC Manager- Handles confirmed major incidents, or attacks attributed to a targeted attacker.
34	NA	NA	Please let us know if the IT security principles/policies/infrastructure and the team managing the function is centralized or decentralized. This needs to be in context all the entities (subsidiaries and manufacturing locations and offices including global entities if any) proposed to be covered under the policy	Security team which is centralized functions under CISO for monitoring the Bank's infra. Bank's CISO is also group CISO for subsidiaries and RRBs for oversight purpose.
36	NA	NA	Have you implemented a procedure to permanently comply with all privacy relevant legislative statutory, regulatory and contractual requirements?	Yes
37	NA	NA	Do you have guidelines issued on the retention, storage, handling and disposal of records and information?	Yes. Archival policy is available.
38	NA	NA	Have you assigned a responsible person for providing guidance and ensuring awareness of privacy principles (e.g. Data Privacy Officer DPO)?	No
39	NA	NA	Do you regularly scan critical systems (incl. penetration tests, vulnerability assessments) - either by yourself or supported by third party? What is the frequency of the scan conducted?	Yes. Extenal VA/PT conducted annulally once through CERT-in empanelled auditors and internal VA is conducted by internal teams on quarterly basis.
40	NA	NA	What is the coverage of VAPT? When was the same last conducted? Was Log4shell and such, also included in the vapt scan conducted if not when would the same be conducted?	We cover all assets of the bank as per policy, For 2021-2022 same was conducted. Log4j vulnerabilities were covered in the same.
42	NA	NA	Information security aspects of business continuity management Have you conducted a Business Impact Analysis (BIA)? When was it last conducted?	Yes. Last Business Impact Analysis (BIA) was conducted for FY 2021-22.

43	NA	NA	Information security aspects of business continuity management Do you have a board approved Business Continuity Management (BCM) plan in place that specifically addresses cyber incidents?	Bank has baord approved BCP policy & Board approved Cyber Crisis Management Plan.
44	NA	NA	Information security aspects of business continuity management Do you test your information security continuity plans (e.g. Business Continuity Management, Disaster Recovery) at least annually?	Yes
45	NA	NA	Information security aspects of business continuity management Are your information processing facilities (i.e. cyber systems, services or cyber infrastructure, or physical location housing it) implemented with redundancy?	Yes
46	NA	NA	Information security aspects of business continuity management Please let us know how a typical BCP testing looks like in terms of Role played by different team and the process	Bank is conducting regular DR drills to ensure robustness of BCP readiness as per Bank's BCP policy.
47	NA	NA	Information security aspects of business continuity management Please let us know how do you arrive at your RTO and RPO?	RTO and RPO are estimated considering Business Impact Analysis and Business continuity reuirements and Technology related controls in place to achieve the same.
48	NA	NA	Information security aspects of business continuity management What is the maximum acceptable outage or also known as RTO (Recovery Time Objective) for cyber systems? Please provide details on the same for critical and non critical systems.	2 hours (for critical systems)
50	NA	NA	Information security incident management Do you have board approved information security incident response plan in place?	Yes.CCMP is in place and is approved by Sub-Committee of the Board - IT
51	NA	NA	Information security incident management Do all your employees and third party providers know the reporting line / escalation procedure for information security events / incidents?	Yes. Bank has communicated through internal circular
52	NA	NA	Information security incident management Are employees and contractors required to report any identified information security weakness (not yet an incident or event) in systems or services?	Yes
53	NA	NA	Information security incident management Do you use knowledge gained from analysing and resolving information security incidents to reduce the likelihood or impact of future information security incidents?	Yes
54	NA	NA	Information security incident management Do you have segregation of network based on Business Function to avoid lateral spread?	Yes

D.I.T. Wing, Procurement Group
CANARA BANK
* H.O. Bengaluru-560 001 *

Replies to the Pre-Bid queries for the GeM Bid Ref No.GEM/2022/B/2894320 dated 22/12/2022 for the "Selection of insurer for renewal of cyber risk insurance policy for Canara Bank from 31st March 2023 to 30th March 2024"

55	NA	NA	Information security incident management Are any data centers / networks / services being shared between the entities / subsidiaries to be covered / or even not covered under the policy please explain in detail?	Not applicable
57	NA	NA	Supplier relationships Have you identified and documented all your important suppliers / vendors (including third party service providers)?	Yes
58	NA	NA	Supplier relationships Do agreements with third party service providers require levels of security commensurate with your own information security standard?	Yes
59	NA	NA	Supplier relationships Do you monitor third party service provider / supplier activities for cyber security events to maintain an agreed level of information security?	Yes.All the systems used by third party service providers working onsite within bank's Corporate network are monitored
61	NA	NA	System acquisition, development and maintenance Does your web-server encrypt confidential data (e.g. HTTPS)?	Yes
62	NA	NA	System acquisition, development and maintenance Do you test security functionality during the development lifecycle of information systems incl. IT security updates? If the response is no. request you to kindly share some more details on this aspect?	Yes
63	NA	NA	System acquisition, development and maintenance Do you consider confidentiality when using operational data for testing to ensure that all sensitive details are protected by removal or modification?	Yes
65	NA	NA	Communications security Are all internet access points secured by appropriately configured firewalls?	Not Applicable. We don't use Internet Access Points.Bank has corporate proxy solution for secure internet access.
66	NA	NA	Communications security Do you monitor your network and identify information security events?	Yes. All the network incidents and events are being monitored by SOC team.
67	NA	NA	Communications security Are all internet-accessible systems (e.g. web-, email-servers) segregated from your trusted network (e.g. within a demilitarized zone (DMZ) or at a 3rd party provider)?	Yes.DMZ and Non DMZ zones are segregated
68	NA	NA	Communications security Do you encrypt confidential communication (e.g. secure emails with SMIME (Secure Multipurpose Internet Mail Extensions) or SMTP-over-TLS (Simple Mail Transfer Protocol Secure))?	Yes. All mail communciations are enabled with TLS 1.2 encryption.

D.I.T. Wing, Procurement Group ★ CANARA BANK ★

69	NA	NA	Communications security Does the organization have network segregation implemented by isolating the demilitarized zone, InterVLAN communications, and Guest VLAN to prevent the movement of an attacker internally in case of a breach? Please explain intervlan security in detail?	Yes. Vlans are created in our datacenter firewall and intervlan access permissions are permittted based on approved CMR process only.
71	NA	NA	Operations security Have you implemented change management procedures for critical systems?	Yes
72	NA	NA	Operations security Is the IT-environment for development and testing separated from production IT-environment?	Yes
73	NA	NA	Operations security Do you use malware protection for all web-proxies, email-gateways, workstations and laptops?	Yes. However not applicable for web proxy.
74	NA	NA	Operations security Besides traditional signature-based detection, does your malware protection use advanced heuristic- and behavioural-based detection mechanisms to protect against new malwares?	Yes
75	NA	NA	Operations security Do you perform at least weekly regular backups of business critical data? Please explain in detail the backup strategy being used in the organisation?	Yes. As per Backup policy/Guidelines.
76	NA	NA	Operations security Do you produce and regularly review event logs recording user activities, exceptions, faults and information security events (at least from your firewalls and domain controller) ?	Yes. All the firewall traffic logs are being sent to SIEM tool.Based on the analysis by SOC team incidents are taken cared with appropriate action.
77	NA	NA	Operations security Have you implemented a centralized software installation process?	Yes
78	NA	NA	Operations security Do you technically or organisationally ensure that employees must not install and, or run unauthorised portable softwares on their workstations? (Please share controls present excluding admin right restrictions being implemented)	Yes. Only whitelisted applications are allowed to install which are controlled through DMS.
80	NA	NA	Physical and environmental security Do you maintain a list of personnel (employees, vendors and visitors) with authorized access to your premises and sensitive security areas?	Yes

D.I.T. Wing, Procurement Group
CANARA BANK
H.O. Bengaluru-560 001

82	NA	NA	Cryptography Is all confidential information stored on mobile devices (e.g. smart phones, laptops) fully encrypted? If No, please elaborate.	Yes. All laptops connected to Bank's network are enrolled with MDM solution
83	NA	NA	Cryptography Have you developed and implemented a policy on the use, protection and lifetime of cryptographic keys?	Yes. The same is as part of IS Policy
85	NA	NA	Access control Do you restrict employees and external users privileges on a business-need to know basis (particularly administrative permissions, access to sensitive data e.g. personal data, etc.)?	Yes
86	NA	NA	Access control Do you have a formal access provisioning process in place for assigning and revoking access rights?	Yes
87	NA	NA	Access control Do you prohibit local admin rights on workstations for employees?	Yes
88	NA	NA	Access control Do you review user access rights at least annually?	Yes
89	NA	NA	Access control Do you revoke all system access, accounts and associated rights after termination of users (incl. employees, temporary employees, contractors, vendors, etc.)?	Yes.
90	NA	NA	Access control	Yes. Password policy is part of IS Policy.
91	NA	NA	Access control Do you have PIM, PAM solution in place? If yes, please specify details including coverage of the solution being used?	Yes.PIM solution is in place
92	NA	NA	Access control Is multi factor authentication being used for all the cyber systems & services? If no what is coverage of the same in the organisation?	Yes
93	NA	NA	Access control Are any of the manufacturing / logistic / generation systems / medical equipments. Either connected or dependant on IT systems which if not working might result in any loss?	Not Applicable

D.I.T. Wing, Procurement Group ★ H.O., Bengaluru-560001 ★ CANARA BANK

95	NA	NA	Asset management Do you keep an up-to-date inventory of software (incl. operating systems) and hardware assets being used in the organisation?	Yes
96	NA	NA	Asset management Do you classify information, data with regards to confidentiality?	Yes
97	NA	NA	Asset management Are information labelling procedures implemented in accordance with the above information classification scheme?	Yes
98	NA	NA	Asset management Do you provide guidance on how to handle classified information?	Yes
99	NA	NA	Asset management Do you either restrict access to, or encrypt confidential information stored on removable media like external storage devices (e.g. USB sticks or hard disks)?	Yes
100	NA	NA	Asset management Do you securely dispose media containing sensitive information if it is not used any longer or if it needs to be disposed?	Yes
101	NA	NA	Asset management	No
103	NA	NA	Human resource security Do you provide at least annual education to increase your users (employees and contractors) security awareness and prepare users to be more resilient and vigilant against phishing or cyber attacks?	Yes.Information Security Awareness is being conducted to all staff members of the Bank. Also, Cyber Security is covered in all the training programmes conducted by Staff Training College with duration of 3 days or more. Phishing simulation exercise is carried out quarterly.
104	NA	NA	Human resource security Do you have any User Behavioural Analytics tool (i.e. UEBA, etc.) to monitor patterns of human behaviour to detect anomalies from those patterns? Please explain in detail?	No
106	NA	NA	Organization of information security Have you assigned a responsible person for information security (e.g. Chief Information Security Officer "CISO")?	Yes

D.I.T. Wing, Procurement Group
CANARA BANK
H.O. Bengaluru-560 001

107	NA	NA	Organization of information security Do you have an up to date list of authorities and external contacts, which must be informed in case of an information security incident?	Yes
108	NA	NA	Organization of information security Please list all the information security functions that exists (within the organization, via external vendor, MSP) to manage/perform day-to-day security tasks, functions (example: SOC, TI, IR, etc.)	IS functions include: 1. 24*7 monitoring of following security solutions implemented in SOC - SIEM, DLP, NBA, Anti-DDoS, Deception, PIM 2. Incident response and management 3. Quarterly internal VA 4. Annual external VAPT by Cert-in empaneled vendor 5. Red Team 6. DAST 7. Threat Hunding 8. Quarterly Table Top Exercise & Drill 9. Quarterly Phishing Simulation Exercise 10. Cyber Security Awareness 11. Action on Threat Intel Feeds received from CSITE, Cert-In, NCIIPC, IB-Cart, & RSA Feeds 12. Regulatory Compliance
109	NA	NA	Organization of information security Are any SaaS services being used, or provided? If yes who is responsible for the protection of data stored on the SaaS service? Please name the service provider being used?	Yes. Microsoft O365.
110	NA	NA	Organization of information security Please share future plans / roadmap for improving cyber security architecture including time frames to implement if any?	New projects under pipeline for improving Bank's cyber security architecture includes: 1. Data Classification Solution 2. Breach & Attack Simulation 3. AD Assessor Solution 4. Endpoint Detection & Response
112	NA	NA	Information security policies Have you documented and implemented a board approved information security policy which is corporate-wide and permanently available for all employees and relevant external parties?	Yes
113	NA	NA	Information security policies Has the organization documented and implemented a board approved cloud security policy to ensure cyber security requirements are catered to when utilizing cloud services for business?	No. Bank is in the process of preparing Cloud security Policy
115	NA	NA	Technology implementation	Yes. As per patch management SOP and policy of the Bank.

D.I.T. Wing, Procurement Group
CANARA BANK
★ H.O., Bengaluru-560 001 ★

116	NA	NA	Technology implementation Does the organization ensure that the default passwords on all computer systems (e.g. routers, etc) are changed to prevent entry in the organizations systems, networks through a brute force attack?	Yes
117	NA	NA	Technology implementation Does the organisation ensure high availability of business critical cyber infrastructure to ensure business continuity in case of an cyber incident?	Yes
118	NA	NA	Technology implementation	Bank has one DC and DR & Near DR Sites. Last DR drill was conducted on 19 Nov 2022.
119	NA	NA	Technology implementation	Yes. Bank has a dedicated inhouse SOC working 24*7
120	NA	NA	Technology implementation	Yes
121	NA	NA	Technology implementation Has the organization implemented Deception Tool, or Honeypot solution to divert and detect attackers with no risk to real data, operations, or users?	Yes
122	NA	NA	Technology implementation Has the organization implemented host-based firewall solution on end-user systems and servers to actively identify and mitigate malicious traffic incoming and outgoing from assets?	Yes, HIPS is implemented in end-users and servers as part of Anti virus solutions.
123	NA	NA	Technology implementation Has the organization implemented an Endpoint threat Detection and Response (EDR) solution on all end point systems and servers to actively monitor and detect security threats based on system behaviour? Such as crowdstrike falcon EDR, etc.	Yes, EDR is a part of Anti virus solution.
124	NA	NA	Technology implementation	Yes. Execution of any software/ programs are controlled centrally through Desktop Management Solution.
125	NA	NA	Technology implementation Has the organization implemented a Intrusion Detection and Prevention (IDS/IPS) solution for network, and host based on all end point systems to detect or prevent any malicious activity on IT assets by monitoring the network traffic?	Yes

D.I.T. Wing Procurement Group ★ CANARA BANK ★ H.O. Bengaluru-560 001

126	NA	NA	Technology implementation Has the organization implemented a Data Leakage Prevention (DLP) tool on all end point systems and servers in blocking mode for making sure that end users do not send sensitive or critical information outside the corporate network?	End point DLP is in block mode and DLP is not implemented in Servers.
127	NA	NA	Technology implementation	Yes, NGFWs with IPS are available
128	NA	NA	Technology implementation Does the organization ensure only secured connections like VPN are utilized by remote users to ensure the confidentiality of sensitive information in transit?	Yes
129	NA	NA	Technology implementation	Yes
130	NA	NA	Technology implementation Has the organization implemented a Database Activity Monitoring (DAM) Solution to detect and prevent malicious behaviour in the database?	Yes
131	NA	NA	Technology implementation Has the organization implemented anti-Distributed Denial-of-Service (DDoS) solution to prevent DDoS attacks?	Yes
132	NA	NA	Technology implementation Please elaborate in details. What is the frequency of backup? How are backups taken?.What is the backup coverage including backup strategy?	Yes, Backup is obtained at regular intervals as per backup policy/Guidelines.
133	NA	NA	Technology implementation	Yes. Systems installed with AV are regualrly updated with latest AV Definitions.
134	NA	NA	Technology implementation When were the WAF rules last updated? Were rules added to WAF solution, to prevent log4j vulnerabilities from being exploited? Please respond in details.	WAF rules are being updated on daily basis. Yes, necessary signature are in place to prevent log4j vulnerabilities.
135	NA	NA	Technology implementation Are any apache, or applications based on java being used in the organisation? When were all of the apache, or applications based on java last updated to the latest version available?	Yes. Upgradations and updating are being done regularly
137	NA	NA	System Failure Operational recovery procedure: description of the existing back-up procedures and capabilities?	Backups are obtained at regular intervals as per the Bank's Backup Policy

D.I.T. Wing, Procurement Group
CANARA BANK
H.O., Bengaluru - 560 001

138	NA	NA	System Failure Existing patching process and procedure in case patching process for IT/OT assets fails? Please describe the rollback procedure in the event a failure happens once implemented into production?	Patching process is as per Bank's policy/SOP.
139	NA	NA	System Failure What redundancies are leveraged in the design of your infrastructure ? (E.g., automatic failover logic, multiple processors, redundant I/O modules, Dual trinked networks)	All Critical Applications are implemented in High Availability in DC & DR. NDR is available for few critical applications.
140	NA	NA	System Failure Do you test updates and upgrades of firmware, software, web-applications and products of your systems before deployment?	Yes
141	NA	NA	System Failure What kind of redundancies do you leverage for your mission critical systems? Are you on a hot or warm site standby?	All Critical Applications are implemented in High Availability in DC & DR. NDR is available for few critical applications.
142	NA	NA	System Failure What kind of Recovery Time Objectives (RTO) do you have for your mission critical systems and are these time objectives tested at least annually?	RTO is 2 hours for most critical applications. DR drill are conducted half yearly to test the RTOs.
143	NA	NA	System Failure Are in house developed software tested prior to deployment into a production environment? If so, do they have rollback procedures in the event a failure happens once implemented into production site?	Yes
144	NA	NA	System Failure Do you have a documented DRP which is tested at least annually? If you leverage SIEM capabilities or equivalent log monitoring, how do such alerts link into your DRP in the event of downtime?	Yes
145	NA	NA	System Failure What redundancies do you leverage in the design of your infrastructure? (E.g. automatic failover logic, multiple processors, redundant I/O modules, dual-trunked networks)	All Critical Application is designed in High Availability. DR and NDR is available in HA
146	NA	NA	System Failure In the absence of a fully redundant primary control system, have you implemented a secondary control system as backup?	Yes. Bank has implemented DR setup for all primary systems
147	NA	NA	System Failure Attached word document questionnaire	Enclosed as a separate Annexure-3

D.I.T. Wing, Procurement Group ★ H.O., Bengaluru-560001 ★ CANARA BANK

148	NA	NA	System Failure Certifications a. Please let us know if you have a ISO 27001 certified ISMS including the Scope b. Let us know the level of your PCI/DSS certification	a.Bank is certified with ISO 27001:2013 certification b.PCI DSS is certified for Card Management System, c.ATM Switch is certified with PA-DSS. d.ATM machines are certified with PA-DSS.
149	NA	NA	System Failure Please let us know if you have implemented data labelling and classification process	Yes
150	NA	NA	System Failure Let us know the details of your encryption process for a. Data at rest b. Data in motion	We are encrypting data at rest using Oracle TDE & storage level encryptions. Data in motion is encrypted using SSL/TLS certificates.
151	NA	NA	System Failure Please share the details of your current SOC setup including a. Scope of their monitoring b. Co-ordination within teams to resolve and update cases c. Please let us know about your SIEM setup.	a) Bank has a dedicated 24x7 SOC supported by System Integrator operating from Bank's premises. SOC is responsible for collecting, maintaining, and regularly reviewing the logs of all network activity and communications for the entire organization along with incident management. b) Proactive threat intelligence gathered from various sources are fed to SIEM for alert generation and thereby preventing occurrence of cyber incidents. c) RSA SIEM solution with DC & DR setup is in place.
152	NA	NA	System Failure Please let us know if you have a CMDB in place which includes inventory of all assets a. If not, let us know how are assets managed	No
153	NA	NA	System Failure Let us know if you have adopted cloud migration for any of your systems and processes a. Please let us know your view on your cloud adoption journey	Bank's email system,elearning applications etc are in cloud. Bank is planning to adopt cloud migration for other applications also as per feasibility and requirement.
154	NA	NA	System Failure Please let us know details of your VAPT exercise	External VAPT is conducted annually through CERT-in empanelled auditors and internal VA is conducted by internal team on quarterly basis
155	NA	NA	System Failure Do you have an EDT implemented a. If yes, what is the current scope	For Endpoints, EDR solution is implemented in Symantec AV. For servers End Protection Platform (EPP) is implemented in Trendmicro DSM.
156	NA	NA	System Failure Please let us know a brief overview of your BCM exercise including a. Process b. Teams involved c. Implementation of learnings and closure of gaps	As per the BCP Policy

D.I.T. Wing, Procurement Group
CANARA BANK
H.O. Bengaluru-560 001

157	NA	NA	System Failure Please let us know if you have faced any cyber/security incident over the past year a. If yes, please share the forensic details b. Have you implemented all the recommendation from the expert?	No incident occurred during the current policy period.
158	NA	NA	System Failure On an overall level, please let us know the security improvements over the last 12 months	Bank is continuously implementing necessary security solutions to protect Bank's infra from cyber threats. Some of the improvement are highlighted as below: 1. Threat Intelligence feeds are fed to the Security solutions automatically using STIX & TAXII on real time basis for monitoring purpose. 2. Bank participates in IDRBT Cyber drills and successfully detected all the attacks performed. 3. Bank has implemented SOC Video Wall for effective monitoring. 4. Implemented latest featured Anti-DDoS solution to combat DoS/DDoS attacks. 5. Threat Hunting is performed on the public facing applications in addition to regular VAPT.
159	NA	NA	Awareness Training Does the organization conduct and measure general Information Security Awareness Training in every financial year to ensure all employees are aware of their responsibility towards information security and the cyber threats they might be susceptible to?	Yes. Information Security Awareness is being conducted to all staff members of the Bank. Also, Cyber Security is covered in all the training programmes conducted by Staff Training College with duration of 3 days or more.
160	NA	NA	Phishing Simulation	Yes. Phishing Simulation exercise is conducted quarterly covering all the employees of the bank
161	NA	NA	Role Specific Security Training	Yes. Bank conducts domain specific security training.Table top exercises and drills are also conducted quarterly.
162	NA	NA	Logging and Monitoring Does the organization implement logging and monitoring of all systems or applications that process, transmit or store confidential information to identify any unauthorized security-related activities that may have been attempted or performed?	Yes.
163	NA	NA	Network Segregation Does the organization have network segregation implemented by isolating the demilitarized zone, Management VLAN, and Guest VLAN to prevent the movement of an attacker in case of a breach?	Yes. Bank has network segregation and implemented Demilitarized Zone and other VLANs.Multiple Firewall are in place to filter inbound & outbound traffic (including business partner network)
164	NA	NA	Data Backup on Servers Does the organization perform regular backups of business-critical data on servers to recover such data in cases of breaches, like ransomware attacks?	Yes. Backups are regularly taken as per Bank's backup policy/Guidelines.

[illegible] Wing, Procurement Group ★ CANARA BANK ★ H.O., Bengaluru-560 001

165	NA	NA	Data Restore on Servers Does the organization ensure backups are regularly tested to validate the accuracy and integrity of the data and to verify the ability to restore data as quickly as possible with the least impact?	Yes, we do ensure backups are regularly tested.
166	NA	NA	Incident Reporting, Investigation, and Recovery Does the organization perform Incident Reporting, Investigation and Recovery effectively to ensure the recurrence rate of security events is minimal?	Yes.Bank has Cyber Crisis Management Plan.
167	NA	NA	Vendor Access Control Has the organization implemented the removal of system access, user accounts, and associated access rights as part of the process to terminate the contract of employees, temporary employees, contractors, or vendors?	Yes.
168	NA	NA	Penetration Tests and Red Team Exercises Does the organization conduct regular external penetration tests and red-teaming exercises to test organizational readiness for identifying/ responding quickly to vulnerabilities/attacks?	Yes.
169	NA	NA	User Privilege Management	Yes as per Password policy.
170	NA	NA	Data Backup & Restore on Endpoints	Yes. Backups are carried out regularly as per Backup policy/Guidelines.
171	NA	NA	Patch Management Does the organization timely, i.e. at least monthly, update IT systems and applications to prevent any known vulnerabilities being exploited?	Yes. This is done via Patch Management Process which is carried out as per Patch management policy and SOP
172	NA	NA	Password Creation Policy	Yes. We have password policy as part of IS policy
173	NA	NA	Default Passwords Does the organization ensure that the default passwords on all computer systems (e.g. routers) are changed to prevent entry in the organization network through a brute-forcing attack?	Yes.
174	NA	NA	Data Disposal Does the organization ensure effective disposal methods, like shredders, are used for properly disposing of confidential information in order to prevent attacks originating from information gathered by activities like dumpster diving?	Yes. Digital data is safely disposed through degaussing and physical records are disposed by shredding.

D.I.T. Wing, Procurement Group ★ CANARA BANK H.O. Bengaluru-560 001

175	NA	NA	Periodic Audits Does the organization perform a cybersecurity risk assessment prior to conducting business with all third-party vendors and a continual assessment every financial year to identify if all their third-party security requirements are met?	Yes. Required cyber security compliances/certifications are checked during vendor onboarding process.
176	NA	NA	Application Software Security	Yes
177	NA	NA	HA for Business Critical Assets Does the organisation ensure a high availability of business critical infrastructure to ensure business continuity in case of an incident?	Yes. Bank's critical systems are implemented with High availability and redundancy.
178	NA	NA	DR Site Does the organization have a Disaster Recovery (DR) site to allow it to continue business-sensitive operations in the event of a disaster?	Yes.
179	NA	NA	DR Drill Has the organization performed a Disaster Recovery (DR) drill to ensure the effectiveness and efficiency of its disaster recovery plan?	Yes. DR drills are conducted twice a year to ensure the effectiveness and efficiency.
180	NA	NA	Periodic Vulnerability/ Configuration Assessments and Patch Management Does the organization identify and mitigate vulnerabilities and configuration flaws through security assessments conducted at least every financial year?	Yes. VAPT is regularly conducted and known vulnerabilities are fixed immediately.Confguration audits also are conducted half yearly.
181	NA	NA	NOC Does the organization have a dedicated Network Operations Center (NOC) that is capable of monitoring, reporting, investigating and recovering any security incident observed within the organization's network?	Yes. Bank has a dedicated Security Operations Center (SOC) & Network Operations Center (NOC) for network monitoring .
182	NA	NA	Cloud Security Policy Has the organization documented and implemented a cloud security policy to ensure security requirements are catered to when utilizing cloud services for business?	Yes. Bank has Cloud security Policy as part of IS Policy
183	NA	NA	Network & Security Devices Hardening Has the organization implemented security hardening of its network and security devices to reduce the attack surface, giving attackers fewer opportunities to gain a foothold within your IT ecosystem?	Yes.
184	NA	NA	Device Encryption	Yes. We are encrypting data at rest using Oracle TDE & storage level encryptions. Data in motion is encrypted using SSL/TLS certificates.

I.T. Wing, Procurement Group ★ CANARA BANK ★ H.O. Bengaluru-560 001

185	NA	NA	Wireless Security Has the organization implemented strong authentication protocols for wireless networks to prevent wireless security attacks?	Not applicable. Bank does not have corporate wireless network.
186	NA	NA	Asset Inventory Management Does the organization maintain its asset inventory for all software and hardware assets to ensure there are no poorly secured assets unintentionally left within the network?	Yes. Inventory is managed centrally.
187	NA	NA	Browser Protection	Yes.
188	NA	NA	Legacy Systems Does the organization restrict the use of legacy (out of date/end of life) software and/or hardware that is officially not provided with security updates by manufacturers/providers (e.g. Windows XP) to prevent risk arising from legacy systems?	Yes.
189	NA	NA	Application Hardening Has the organization implemented measures to ensure the security hardening of applications, application servers, middleware, and databases to reduce the attack surface, giving attackers fewer opportunities to gain a foothold within your IT ecosystem?	Yes. Configuration audits and VAPT assessments are done to ensure the same.
190	NA	NA	Cloud Services Hardening	Not Applicable
191	NA	NA	System Hardening Has the organization implemented security hardening of its end-user systems and servers to reduce the attack surface, giving attackers fewer opportunities to gain a foothold within your IT ecosystem?	Yes.
192	NA	NA	Network Discovery	Yes. NAC Solution is used for the purpose
193	NA	NA	Network Access Control	Yes. NAC Solution is used for the purpose
194	NA	NA	Enterprise Threat Protection (ETP) Has the organization implemented an Enterprise Threat Protection (ETP) DNS proxy to detect and prevent any malicious activity ingress to the organization?	No
195	NA	NA	Deception Tools & Honeypots Has the organization implemented a Deception Tools & Honeypots solution to divert and detect attackers with no risk to real data, operations, or users?	Yes. Bank has implemented Deception Decoy Technology as part of Security Operations Center solutions using high-interaction deception and decoy technology.

D.I.T. Wing, Procurement Group ★ CANARA BANK ★ H.O., Bengaluru-560 001

196	NA	NA	Host Based Firewall Has the organization implemented host-based firewall solutions on end-user devices and servers to actively identify and mitigate malicious traffic incoming to and outgoing from assets?	Yes. HIPS is implemented in Antivirus solutions of Endpoints & Servers used in our organization.
197	NA	NA	Advanced Persistent Threat (APT)/ EDR Has the organization implemented an Advanced Persistent Threat (APT) solution on end-user devices and servers to actively monitor and detect security threats based on system behavior?	Yes.Server and End-point anti- APT solutions are available.
198	NA	NA	Application Whitelisting Has the organization implemented an application whitelisting solution on end-user devices and servers to limit the use of only authorized licensed applications on the assets?	Yes. Execution of any software/ programs are controlled centrally through Desktop Management Solution in endpoints. For servers, Antivirus application control feature is in place.
199	NA	NA	User Entity Behaviour Analysis Has the organization implemented a User Entity Behavior Analysis (UEBA) solution on end-user devices and servers to detect anomalous behavior and to prevent insider threats/compromised users?	No.
200	NA	NA	Intrusion Detection and Prevention Has the organization implemented a Network-based Intrusion Detection and Prevention (NIDS/NIPS) solution to detect and prevent any malicious activity by monitoring the network traffic?	Yes. Network level IPS is implemented in firewalls for preventing unauthorized connections from external to internal network
201	NA	NA	URL Filtering Has the organization ensured that the standard security configuration of internal firewalls is individually adapted to prevent access to unauthorized external websites?	Yes. Bank has deployed Secure Web gateway Solution(Proxy) for URL filtering.
202	NA	NA	Application Filtering Has the organization ensured that the standard security configuration of internal firewalls is individually adapted to prevent access to unauthorized applications?	Yes. Bank has deployed Secure Web gateway Solution(Proxy) for Application filtering.
203	NA	NA	Data Loss Prevention Has the organization implemented a Data Loss Prevention (DLP) tool in monitor mode for making sure that end users do not send sensitive or critical information outside the corporate network?	End point DLP is in block mode and DLP is not implemented in Servers.
204	NA	NA	Firewall	Bank has deployed NGFW with IPS.
205	NA	NA	Teleworking (VPN) Does the organization ensure only secured connections are utilized for remote users to ensure the confidentiality of sensitive information in transit?	Yes.

D.I.T. Wing, Procurement Group ★ CANARA BANK ★ H.O., Bengaluru - 560 001

206	NA	NA	Security Incident and Event Management Tool Has the organization implemented a Security Incident and Event Management (SIEM) solution for proactively preventing, detecting, analyzing, and responding to security threats that the organization may face in a timely manner?	Yes. SIEM Solution is implemented for proactively preventing, detecting, analyzing, and responding to security threats
207	NA	NA	Privilege Identity and Access Management Has the organization implemented a centralized privileged identity and access management (IAM) solution to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications?	Yes. PIM is implemented for servers and AD is in place for endpoints.
208	NA	NA.	Mobile Device Management Has the organization implemented a Mobile Device Management (MDM) solution to monitor, manage, and secure employee's mobile devices?	Yes. MDM is enabled for laptops used to access bank's network.
209	NA	NA	Database Activity Monitoring Has the organization implemented a Database Activity Monitoring (DAM) Solution to detect and prevent malicious behavior in the database?	Yes. DAM is implemented
210	NA	NA	Network Behaviour Anomaly Detection (NBAD) Has the organization implemented a Network Behaviour Anomaly Detection (NBAD) solution to continuously monitor the network for unusual events or trends that indicate a threat to the organization?	Yes. NBA is implemented. NBA performs behavioural analysis, identifies applications and protocols to optimize security, network operations, and application performance.
211	NA	NA	Web Application Firewall Has the organization implemented a Web Application Firewall (WAF) capable of preventing the exploitation of web application vulnerabilities covering at least OWASP's Top 10 threats?	Yes. Web Application Firewall (WAF) is implemented for all the Public facing applications
212	NA	NA	Host Intrusion Prevention System Has the organization implemented a host-based intrusion detection and prevention solution (HIDS/HIPS) on end-user devices and servers to detect and prevent any malicious activity on assets?	Yes. HIPS is implemented in Antivirus solutions of Endpoints & Servers used in our organization.
213	NA	NA	Configuration Management Tool Has the organization implemented a Configuration Management Solution (CMS) to conduct regular configuration security assessments on all organization-owned assets?	Yes
214	NA	NA	Load Balancer Has the organization implemented a Load Balancer to maintain the availability of critical resources?	Yes

D.I.T. Wing, Procurement Group ★ CANARA BANK ★ H.O., Bengaluru-560 001

215	NA	NA	DDOS Prevention Has the organization implemented anti-Distributed Denial-of-Service (DDoS) solutions to prevent DDoS attacks?	Yes.
216	NA	NA	Vulnerability Management Tool Has the organization implemented a Vulnerability Management Solution (VMS) to conduct regular Vulnerability Assessment and Penetration Testing (VAPT) security assessments on all organization-owned assets?	Yes
217	NA	NA	Patch Management Tool Has the organization implemented a patch management solution to ensure that all critical and high-risk vulnerabilities reported are patched or mitigated within two days?	Yes. Patch management is ensured as per SOP and laid down policy.
218	NA	NA	Anti-Malware Has the organization implemented anti-malware or equivalent protection on end-user devices and servers that are updated/patched as per the vendor's recommendations to prevent malicious software attacks (e.g. IT virus, ransomware, spyware, etc.)?	Yes. Bank has implemented Trend Micro and Symantec AV solutions for the purpose.
219	NA	NA	Company Information Number of employees in the previous financial year	86,919 (As on 31.03.2022)
220	NA	NA	Company Information Number of employees in the current financial year	85,576 (As on 01.01.2023)
221	NA	NA	Company Information Number of employees for the projected financial year	84,000 (Projected figures for 31.03.2024)
222	NA	NA	Company Information Number of online customers in the previous financial year	6,05,82,959 (As on 05-05-2022)
223	NA	NA	Company Information Number of online customers in the current financial year	6,70,23,751 (As on 09-01-2023)
224	NA	NA	Company Information Number of online customers for the projected financial year	Cannot be provided
225	NA	NA	Turnover/ Revenue, US assets, websites Gross revenue in the previous financial year	85,907.15 Crores INR
226	NA	NA	Turnover/ Revenue, US assets, websites Gross revenue in the current financial year	48,284.15 Crores INR
227	NA	NA	Turnover/ Revenue, US assets, websites Gross revenue for the projected financial year	Cannot be provided

I.T. Wing, Procurement Group
CANARA BANK
H.O., Bengaluru-560 001

228	NA	NA	Organization's Attack History	Please refer to the claim note enclosed as Annexure-4.
229	NA	NA	Organization's Attack History If the answer to the above question is yes, how many incidents did the software or hardware malfunction cause the network (or any portion thereof) to stop operating totally or failed to start operating without any human intervention?	Please refer to the claim note enclosed as Annexure-4.
230	NA	NA	Organization's Attack History What were the primary causes of the hardware or software malfunctions?	Please refer to the claim note enclosed as Annexure-4.
231	NA	NA	Organization's Attack History What was the highest total cost incurred (not including standard staff time and other regular operating expenses) to rectify the malfunction and bring the critical system(s) back online?	Please refer to the claim note enclosed as Annexure-4.
232	NA	NA	Organization's Attack History Please mention the measures taken by the organization to prevent the reoccurrence of the issue/ breach faced.	Not Applicable.
233	NA	NA	Organization's Attack History What actions did the organization take to recover the applications, data, or cost of recovery?	Not Applicable.
234	NA	NA	Organization's Attack History How long did the organization take to restore the affected applications/ operations?	Not Applicable.
235	NA	NA	Organization's Attack History Please provide comments on the exposure of Proprietary & Confidential data that the organization host, store, share, transmit, publish, or transact.	Proprietary and Confidential information of customers as necessary for various buinsess transactions is held by the Bank
236	NA	NA	Organization's Attack History Please provide comments on the exposure of published electronic content.	Bank publishes business related content applicable to its operations and as required under various regulatory requirements on its website. Bank's website www.canarabank.com may be referred for illustrations.
237	NA	NA	Organization's Attack History Please provide comments on the exposure of Web-enabled transactions.	Bank has various web aplications for servicing to customers eg.Net banking, Mobile Banking etc.
238	NA	NA	Organization's Attack History Please provide comments on the exposure of Consumer Identity Theft, including remediation for notification costs.	Bank's processes and stores Customer PII data and adequate protection measures are in place to prevent any such incidents.

D.I.T. Wing, Procurement Group
CANARA BANK
H.O. Bengaluru-560 001

239	NA	NA	Organization's Attack History Please provide comments on the possible service disruption, mainly if operations are contingent upon technology platforms.	Customer service may be disrupted and branches and online channels.
240	NA	NA	Organization's Services to Third Parties Does the organization provide technology services or products to third parties?	Yes. Bank processes card Payments on behalf of RRBs/Grameen Banks (i.e. Karnataka Grameen bank , Kerala Grameen Bank, Andhra Pragathi Grameena Bank & Karnataka Vikas Grameena Bank)
241	NA	NA	Organization's Services to Third Parties Do third parties rely on the availability of the organization's technology platforms (such as website(s), data processing services, hosting services, internet transactions, etc.) to transact business?	Yes. Bank processes card Payments on behalf of RRBs/Grameen Banks (i.e. Karnataka Grameen bank , Kerala Grameen Bank, Andhra Pragathi Grameena Bank & Karnataka Vikas Grameena Bank)
242	NA	NA	Organization's Services to Third Parties	RRBs/Grameena Banks are utilising Parent Bank's ATM Switch services only. No businnes revenue is dependent on parent Bank's ATM Switch platform.
243	NA	NA	Criticality Based on Data Consumption Does the organization process credit/ debit card information, including merchants or third party service providers which store, process, or transmit credit/ debit card data?	Yes.
244	NA	NA	Criticality Based on Data Consumption Is the organization Payment Card Industry (PCI) compliant?	Yes.
245	NA	NA	Organization's Attack History Was the organization targeted explicitly for computer attacks?	No.
246	NA	NA	Organization's Attack History If the organization was targeted explicitly for computer attacks, what were the direct costs associated with all the computer attacks?	Not Applicable.
247	NA	NA	Organization's Attack History If the organization was targeted explicitly for computer attacks, have any of the computer attacks resulted in unauthorized access, corruption, or deletion of data?	No incident occurred during the current policy period.
248	NA	NA	Organization's Attack History Has the organization encountered a security breach that required notifications to customers or other third parties?	No.
249	NA	NA	Organization's Attack History How long has the organization continuously carried on business?	Bank is in the business for 117 years
250	NA	NA	Organization's Attack History Does the Security Incident Response Plan include a review by the organization's legal counsel of laws or regulations that may affect the organization's response or other standards to which the organization may have to comply?	Yes. Bank has Cyber Crisis Management Plan complies with required regulatory obligations.

I.T. Wing, Procurement Group ★ CANARA BANK ★ H.O. Bengaluru-[illegible]

251	NA	NA	Organization's Attack History Has the Security Incident Response Plan been reviewed and approved by the organization's Board of Directors or persons with substantially similar responsibilities?	Yes. Approved by Board of directors.
252	NA	NA	Organization's Attack History Has the organization faced any computer or network security incidents in the past two years?	No.
253	NA	NA	Organisation's Claim History Has the organization ever been refused for cybersecurity or similar insurance, or had a similar policy cancelled?	No.
254	NA	NA	Organisation's Claim History Does the organization currently have cyber security or similar insurance? Please enter the limits and other details of the insurance..	Yes. Limit is 450 Cr
255	NA	NA	Organisation's Claim History Does the organization conduct a test for the IT Security Incident Response Plan and address the issues identified at least annually?	Yes. Plan is in place and reviewed annually
256	NA	NA	Data Backup on Servers Operational recovery procedure: description of the existing back-up procedures and capabilities?	Yes. A documented backup procedure is in place for both the application and the database to ensure IT continuity and data resilience. Daily / weekly / monthly / quarterly and yearly backups are executed based on this and off-site storage maintained to ensure adequate data resilience. The backup is taken according to the laid down policy
257	NA	NA	Patch Management Existing patching process and procedure in case patching process for IT/OT assets fails? Please describe the rollback procedure in the event a failure happens once implemented into production?	Yes. For desktops & servers, Regular patches are being applied on N-1 basis which is in tune with industry best practices and critical/high risk patches are deployed immediately. For Servers, we use Virtual Patching method also to mitigate the Zero-day vulnerabilities.
258	NA	NA	Redundancy of IT infrastructure What redundancies are leveraged in the design of your infrastructure ? (E.g, automatic failover logic, multiple processors, redundant I/O modules, Dual trinked networks)	Yes. All Critical Applications are designed in High Availability. DR and NDR is available in HA
259	NA	NA	Redundancy of IT infrastructure Do you test updates and upgrades of firmware, software, web-applications and products of your systems before deployment?	Yes.
260	NA	NA	Redundancy of IT infrastructure What kind of redundancies do you leverage for your mission critical systems? Are you on a hot or warm site standby?	Yes. All Critical Applications are designed in High Availability. DR is on hot site

D.I.T. Wing, Procurement Group
CANARA BANK
H.O. Bengaluru-560 001

261	NA	NA	Recovery time of critical systems What kind of Recovery Time Objectives (RTO) do you have for your mission critical systems and are these time objectives tested at least annually?	Yes. Recovery Time and Recovery Point objectives have been defined and approved by the management. These are annually tested and the results are well within the approved RTO & RPO
262	NA	NA	Recovery time of critical systems Are in house developed software tested prior to deployment into a production environment? If so, do they have rollback procedures in the event a failure happens once implemented into production site?	Yes. Software development life cycle process is in place for all application deployment
263	NA	NA	Does the company have Board approved Information Security & privacy policy and it is communicated to all stakeholders? Please confirm which option is applicable Ø No information policy is present Ø ISP is present but not approved by board Ø ISP is present & approved by board Ø Approved Policy is in place but not communicated to all stakeholders Ø Policy is in place and communicated to all stakeholders	Ø IS Policy is present & approved by board
264	NA	NA	Does the company have Board approved Incident Response Plan, Disaster recovery plan, Business Continuity plan and are they reviewed at least annually? Please confirm which option is applicable Ø No, Incident Response, Business Continuity plan, Disaster recovery plan are not present Ø IR/BC/DR is present but not approved by board Ø IR/BC/DR is present & approved by board Ø Approved Disaster recovery plan, Business Continuity plan are present but not reviewed Annually Ø Approved Disaster recovery plan, Business Continuity plan are present and are reviewed Annually	Ø IR/BC/DR is present & approved by board Ø Approved Disaster recovery plan, Business Continuity plan are present and are reviewed Annually
265	NA	NA	Mention the duration in which the company likely to incur a loss of profit after a cyber-attack? Please confirm which option is applicable Ø 1-12 Hours Ø 12-24 Hours Ø 24 to 36 Hours Ø 36 to 48 Hours Ø 48 Hours and above	Details will be shared with the selected bidder
266	NA	NA	Has your organization been compromised in past?	No such security breach incident reported during current policy period.
267	NA	NA	Which are the information security certification hold by your organization? Please confirm which option is applicable Ø ISO 27001 Ø PCI DSS Ø ISO 27004 Ø ISO 22301 Ø ISO 27017 Ø SOC2 Ø None Ø Please mention if any other	Ø ISO 27001

D.I.T. Wing, Procurement Group ★ CANARA BANK

268	NA	NA	What is the impact/severity in terms of daily loss of profit after cyber attack or interruption in company's IT network?	Business impact analysis is carried out as per Bank's internal BCP policy.
269	NA	NA	**Does the Company conduct regular Review/Audit of the consultant and third party service providers to ensure that they meet the company's requirement for critical data in their custody?** Ø Data is shared but Audit is never conducted Ø Review/Audit is done only at the time of on boarding Ø Audit/Review is conducted at least once in two years Ø Audit/Review is conducted at least once a year Ø Not applicable as company do not share critical info with any other third party	Ø Not applicable as company do not share critical info with any other third party
270	NA	NA	Does it require to comply with data protection laws applicable to jurisdictions in which company operates?	Bank does not have an exclusive Data protection policy. However, few Data protection requirements as per IT Amendment Act 2008 & Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules 2011 (IT RSPPSPI Rules) are mentioned as part of Information Security Policy. For Foreign branches, Bank is having separate policies in compliance with host country regulations.
271	NA	NA	Has organization been ever investigated in relation to safeguard of personal information?	No
272	NA	NA	How many cyber security trainings is conducted throughout the year for employees to upgrade security awareness level? (Programs, tests, trainings, phishing mail campaigns) Please confirm which option is applicable Ø No Cyber security trainings are conducted Ø only conducted at the time of joining Ø Conducted once in a year for all employees Ø Conducted Twice in a year for all employees Ø Conducted More than 2 times in a year	Information Security Awareness is being conducted to all staff members of the Bank. Also, Cyber Security is covered in all the training programmes conducted by Staff Training College with duration of 3 days or more.
273	NA	NA	Are security audit logs generated for all hardware and softwares installed on it?	Yes
274	NA	NA	What is the frequency of validation of log reports to uncover the anomalies of Critical System Components? Please confirm which option is applicable Ø No Security Audit Log Report is generated Ø At least monthly Ø At least Fortnightly Ø At least weekly Ø Automated continuous review is schedule	Ø Automated continuous review is schedule
275	NA	NA	Are only fully supported/updated web browsers and email clients allowed to execute in the organization?	Yes
276	NA	NA	Is secure configuration is used for all softwares and hardware (Mobile devices, Laptop, Workstations and servers) including network devices (firewall, router and switch)?	Yes
			How often assessment programs run to determine wheather all systems' softwares & security patches are updated?(including remote access connection) Please confirm which option is applicable	

I.T. Wing Procurement Group
CANARA BANK
H.O. Bengaluru - 560 001

277	NA	NA	Ø No assessment programs are scheduled Ø once in a Fortnight Ø once in a week Ø once in a day Ø Continuous assessment Program is scheduled	Continuous assessment Program is scheduled. Security assessments are conducted as per Bank's policy.
278	NA	NA	Does company have Anti-virus & Firewall installed on computer system? If yes, What is the frequency for updating this? Please confirm which option is applicable Ø Anti virus & Firewall are not installed Ø Updated At least Within a month Ø Updated Within A fortnight Ø Updated Within a Week Ø Updated daily	Ø Updated daily
279	NA	NA	Is comparision of firewall, router and switch configuration against standard for each network devices performed?	Yes. Hardening scans are conducted.
280	NA	NA	Is cyber security assessment performed for all applications before moving into production?	Yes. VAPT & Source code audits are conducted before moving to production.
281	NA	NA	Is any network access control technology in place to authorize authenticated devices and software installation before allowing them on the network? Please confirm which option is applicable Ø No Network Access control Ø Network Access control for Authenticated Devices only Ø Network Access control for Authenticated Software only Ø Network Access control for both Authenticated Software and Devices	Ø Network Access control for Authenticated Devices only
282	NA	NA	How often all the Ports are scanned against all critical servers for to & fro data movement? Please confirm which option is applicable Ø No Scans are performed Ø Monthly Scans Ø Weekly Scans Ø Daily Scans Ø Continuous scanning of key servers	Ø Weekly Scans
283	NA	NA	Does the company have checks in place to identify and detect network security weakness? (internal/External Vulnerability assessment)	VAPT is conducted regulalry for network & security devices of the Datacenters.
284	NA	NA	Any external or internal penetration tests are conducted to identify vulnerabilities or attack vectors? If yes, What is the frequency of penetration tests. Please confirm which option is applicable Ø Never Ø Once in two years Ø Yearly Ø Half Yearly Ø At least Quarterly	Ø Yearly Ø At least Quarterly
285	NA	NA	In case of cyber attack, which multilayer boundary defence are in place to filter inbound and outbound traffic (including business partner network)? Multiple Choice. Please confirm which option is applicable Ø None Ø Stateful firewall/Proxy firewall (Basic) Ø Static packet filter Ø IDS and IPS	Ø NGF(Next gen firewall)/web application firelwall

D.I.T. Wing, Procurement Group
CANARA BANK
H.O. Bengaluru-560001

			Ø VPN device Ø NGF(Next gen firewall)/web application firelwall	
286	NA	NA	Which type of data organization collect, store & process? (Multiple Choice). Please confirm which option is applicable Ø Financial/Credit/Payment Card Data Ø Medical/Healthcare Ø Personal Identity Data Ø Business(corporate Info) Ø None of the above	Ø Financial/Credit/Payment Card Data Ø Personal Identity Data
287	NA	NA	What is the frequency of Data Back Up(Operating System, Application Software and Data)? Please confirm which option is applicable Ø Never Ø Monthly Ø Fortnightly Ø Weekly Ø At least twice in a Week	Yes. Daily / weekly / monthly / quarterly and yearly backups are executed according to the laid down policy.
288	NA	NA	How many times data restoration process is verified to ensure back up data is properly working? Please confirm which option is applicable Ø Never Ø Half yearly Ø Quarterly Ø Monthly Ø Fortnightly Ø Weekly	Ø Half yearly
289	NA	NA	Is data in stored form(On Cloud, Servers,Laptops,flash drives, back up tapes) or in transit form, encrypted using strong encryption technologies? Please confirm which option is applicable Ø No encryption technology is used Ø Data in stored form only is encrypted Ø Data in stored form and in transit form is encrypted	Ø Data in stored form and in transit form is encrypted
290	NA	NA	Are data access restrictions inforced on the basis of specific role rights ?	RBAC acess restrictions are enabled as per requirements to access data.
291	NA	NA	How many times Admin access rights are reviewed to ensure only that only administrative functions (Non-Internet Connection based) are performed on those systems? Please confirm which option is applicable Ø No review is performed on administrative account Ø Yearly Ø Quarterly Ø Monthly Ø Fortnightly	Ø Monthly
292	NA	NA	Which user access management methods are being used in your organization? (Multiple Choice) Please confirm which option is applicable Ø Disable account that is not associated with any business owner & process Ø Revoking system access immediately after termination Ø Strong Password policy with unique, complex & with expiration date Ø Screen locks on unattended systems	▫ Disable account that is not associated with any business owner & process ▫ Revoking system access immediately after termination ▫ Strong Password policy with unique, complex & with expiration date ▫ Screen locks on unattended systems ▫ Lockouts after a set number of failed login attempts ▫ Clear Desktop Policy

I.T. Wing, Procurement Group ★ CANARA BANK ★ H.O., Bengaluru-560 001

			Ø Lockouts after a set number of failed login attempts Ø Clear Desktop Policy	
293	NA	NA	Does company have security controls in place to authenticate all user(including remote user and wireless area) before being allowed to connect to internal network and computer system?	YES
294	NA	NA	Please share information security policy, RTO in case of IT infra failure	Bank is having board approved Information Security Policy. RTO is 2 hrs for critical systems as per BCP Policy of the Bank
295	NA	NA	Is SOC empowered to perform continuous data monitoring?	There is no data monitoring performed in SOC. Only Security events and log monitoring is in place.
296	NA	NA	Which EDR solution is installed on all end points?	Symantec EDR is in place for End points.
297	NA	NA	Is financial messaging systems (NIFT/SWIFT) is audited regularly?	Yes, SWIFT Messaging System Audited Regularly
298	NA	NA	Please share claim details under existing Cyber Policy ending on 30th March 2023	Please refer to the claim note enclosed as Annexure-4.
299	NA	NA	Please confirm Current status of claim along with Admissibility status along with Claim Reserve Created by Insurer	Please refer to the claim note enclosed as Annexure-4.
300	NA	NA	Please share Corrective measures taken by the client to prevent occurence in future.	Required controls measures have been implemented to prevent such incidents.
301	NA	NA	Please share Policy Copy for Policy Period from 31st March 2022 to 30th March 2023	Policy document can not be shared. Please refer to Scope of cover and policy wordings which were part of last year's tender document.
302	NA	NA	Does the Insured have End point Solutions in Place ?	YES
303	NA	NA	Does the Insured have a Behavorial based end point?	YES
304	NA	NA	Has your organisation undertaken a Phishing Campaign on Peroidic basis	YES
305	NA	NA	What percentage of your employees fell for the trap in your Phishing Campaign?	0.73%

Date:12/01/2023
Place:Bangalore

Deputy General Manager

S.I.T. Wing, Procurement Group
CANARA BANK
H.O. Bengaluru-560001

ANNEXURE - I

Cyber Risk Protector Supplemental Questionnaire - Ransomware

This Supplemental Questionnaire is applicable to Cyber Risk Protector coverage. As used herein, "**Applicant**" includes the **Company** applying for Cyber Risk Protector coverage and its subsidiaries.

Note: Response boxes shaded this color require an individual selection, effectively, which response option best
Response boxes shaded this color represent questions where multiple responses may be selected. Note, these

Full Name of Applicant:	

1	With respect to the Applicant's efforts to mitigate phishing, <u>select all that apply</u>	
	Applicant provides security awareness training to employees at least annually.	X
	Applicant uses simulated phishing attacks to test employees' cybersecurity awareness at least annually.	X
	Where the Applicant is conducting simulated phishing attacks, the success ratio was less than 15% on the last test (<u>less than 15%</u> of employees were successfully phished).	X
	Applicant 'tags' or otherwise marks e-mails from outside the organization.	X
	Applicant has a process to report suspicious e-mails to an internal security team to investigate.	X
	None of the above.	
	Additional Commentary on efforts to mitigate phishing:	
2	Does the Applicant have a documented process to respond to phishing campaigns (whether targeted specifically at the Applicant or not)?	
	Yes	X
	No	
	If "Yes", please describe the principal steps to respond:	
3	With respect to the **Applicant's** efforts to block potentially harmful websites and/or email, <u>select all that apply:</u>	
	Applicant uses an e-mail filtering solution which blocks known malicious attachments and suspicious file types, <u>including executables</u>.	X
	Applicant uses an e-mail filtering solution which blocks suspicious messages based on their content or attributes of the sender.	X
	Applicant uses a web-filtering solution which stops employees from visiting known malicious or suspicious web pages.	X
	Applicant uses block uncategorized and newly registered domains using web proxies or DNS filters.	X
	Applicant uses a web-filtering solution which blocks known malicious or suspicious downloads, <u>including executables</u>.	X
	Applicant's e-mail filtering solution has the capability to run suspicious attachments in a sandbox.	X
	Applicant's web filtering capabilities are effective on all corporate assets, even if the corporate asset is not on a corporate network (e.g. assets are configured to utilize cloud-	
	None of the above.	
	Additional commentary on efforts to block malicious websites and/or email:	
4	With respect to authentication for <u>employees</u> who are remotely accessing the corporate network and any cloud-based services where sensitive data may reside (including	
	Remote access to corporate resources requires a valid username and password (single factor authentication).	
	Multi-factor authentication is in place for some types of remote access to corporate resources, but not all.	
	Multi-factor authentication is required by policy for all remote access to corporate resources; all exceptions to the policy are documented.	X
	Applicant does not provide remote access to employees.	
	Additional commentary on authentication for employees:	

I.T. Wing, Procurement Group
CANARA BANK
★ H.O. Bengaluru-560 001 ★

5	With respect to authentication for independent contractors and vendors who are remotely accessing the corporate network and any cloud-based services where sensitive	
	Remote access to corporate resources requires a valid username and password (single factor authentication).	
	Multi-factor authentication is in place for some types of remote access to corporate resources, but not all.	
	Multi-factor authentication is required by policy for all remote access to corporate resources; all exceptions to the policy are documented.	X
	Applicant does not provide remote access to independent contractors/vendors.	
	Additional commentary on authentication for independent contractors/vendors:	
6	Does the **Applicant's** multifactor authentication implementation also meet the criteria that the compromise of any single device will only compromise a single authenticator?	
	Not Applicable (**Applicant** does not use multi-factor authentication)	
	No; **Applicant's** multi-factor implementation does not meet the above criteria.	
	Yes; the **Applicant's** multi-factor implementation meets the above criteria.	X
	Additional commentary on Multi-factor authentication implementation:	
7	With respect to the **Applicant's** endpoint security of workstations (desktops and laptops), select all that apply:	
	Applicant's policy is that all workstations have antivirus with heuristic capabilities.	X
	Applicant uses endpoint security tools with behavioral-detection and exploit mitigation capabilities.	X
	Applicant has an internal group which monitors the output of endpoint security tools and investigates any anomalies.	X
	None of the above.	
	Additional commentary on endpoint security capabilities:	
8	With respect to monitoring the output of security tools, select the description which best reflects the **Applicant's** capabilities: (The Applicant can provide further explanation	
	Applicant does not have staff dedicated to monitoring security operations (a "**Security Operations Center**").	
	Applicant has a **Security Operations Center**, but it's not 24/7 (can be internal or external).	
	Applicant has a 24/7 monitoring of security operations by a 3rd party (such as a Managed Security Services Provider).	
	Applicant has 24/7 monitoring of security operations internally.	X
	Additional commentary on security monitoring:	
	Bank's Reply: Canara Bank Cyber Security Operations Centre (CSOC) is an organized and highly skilled team whose mission is to continuously(24 X 7) monitor and improve the organization's cybersecurity posture while preventing, detecting, analysing and responding to security incidents with the aid of technology and well-defined processes and procedures. SOC performs continuous monitoring of Bank's IT assets through analysis of incidents reported by Security Information & Event Management (SIEM) solution to guard against Information Security breaches and incidents to have a real-time/near-real time information on the insight into security posture of the Bank.	
9	What is the **Applicant's** average time to triage and contain security incidents of workstations year to date? (The Applicant can provide further explanation below)	
	Applicant does not track this metric/Do not know	X
	<30 minutes	
	30 minutes-2 hours	
	2-8 hours	
	>8 hours	
	Additional commentary on average time to remediate:	

D.I.T. Wing, Procurement Group ★ H.O., Bengaluru-560 001 ★
CANARA BANK

10	With respect to access controls for each user's workstation, select the description which best reflects the **Applicant's** posture:	
	No employees are in the Administrators' group or have local admin access to their workstations.	
	Applicant's policy is that employees by default are not in the Administrators' group and do not have local admin access; all exceptions to the policy are documented.	X
	Some of **Applicant's** employees are in the Administrators' group or are local admins.	
	Do not know.	
	Additional commentary on access controls for workstations:	
11	With respect to protecting privileged credentials, select all that apply with respect to the **Applicant's** posture:	
	System administrators at the **Applicant** have a unique, privileged credential for administrative tasks (separate from their user credentials for everyday access, email, etc.).	X
	Privileged accounts (including Domain Administrators) require multifactor authentication.	X
	Privileged accounts are kept in a password safe that require the user to "check out" the credential (which is rotated afterwards).	
	There is a log of all privileged account use for at least the last thirty days.	X
	Privileged Access Workstations (workstations that do not have access to internet or e-mail) are used for the administration of critical systems (including authentication	X
	None of the above.	
	Additional commentary on protecting privileged credentials:	
12	Indicate the **Applicant's** use of Microsoft Active Directory (across all domains/forests):	
	Applicant does not use Microsoft Active Directory (indicate to the right)	
	Number of user accounts in the Domain Administrators group (include service accounts - if any - in this total):	10
	Number of service accounts in the Domain Administrators group:	4
	Additional commentary on the number of Domain Administrators:	
13	How many users have persistent privileged accounts for endpoints (servers and workstations)?	
	Please enter an integer:	1(server)
	Additional commentary on the number of privileged accounts:	
	Bank's reply: Workstations-NIL	
14	With respect to the security of externally facing systems, select all that apply to the **Applicant's** posture:	
	Applicant conducts a penetration test at least annually to assess the security of its externally facing systems.	X
	Applicant has a Web Application Firewall (WAF) in front of all externally facing applications, and it is in blocking mode.	X
	Applicant uses an external service to monitor its attack surface (external/internet facing systems).	X
	None of the above.	
15	What is the **Applicant's** target time to deploy 'critical' – the highest priority – patches (as determined by the **Applicant's** standards for when patches must be deployed)?	
	There is no defined policy for when patches must be deployed.	
	Within 24 hours.	X
	24-72 hours.	
	3-7 days.	
	> 7 days.	
	Additional commentary on target times for patching:	
	Bank's reply: For desktops & servers, Regular patches are being applied on N-1 basis which is in tune with industry best practices and critical/high risk patches are deployed immediately. For Servers, we use Virtual Patching method also to mitigate the Zero-day vulnerabilities.	

D.I.T. Wing, Procurement Group ★ H.O. Bengaluru-560 001 CANARA BANK

16	What is the **Applicant's** year to date compliance with its own standards for deploying critical patches?	
	Applicant does not track this metric/Do not know	
	>95%	X
	90-95%	
	80-90%	
	<80%	
	Additional commentary on patching compliance:	
	Bank's reply: For desktops & servers, Regular patches are being applied on N-1 basis which is in tune with industry best practices and critical/high risk patches are deployed immediately. For Servers, we use Virtual Patching method also to mitigate the Zero-day vulnerabilities.	
17	With respect to the **Applicant's** network monitoring capabilities, select all that apply:	
	Applicant uses a security information and event monitoring (SIEM) tool to correlate the output of multiple security tools.	X
	Applicant monitors network traffic for anomalous and potentially suspicious data transfers.	X
	Applicant monitors for performance and storage capacity issues (such as high memory or processor usage, or no free disk space).	X
	Applicant has tools to monitor for data loss (DLP) and they are in blocking mode.	
	None of the above.	X
	Additional commentary on network monitoring:	
	Bank's reply: Proxy DLP is in learning mode and email DLP is in blocking mode	
18	With respecting to limiting lateral movement, select all that apply to the **Applicant's** posture:	
	Applicant has segmented the network by geography (e.g. traffic between offices in different locations is denied unless required to support a specific business requirement).	X
	Applicant has segmented the network by business function (e.g. traffic between asset supporting different functions – HR and Finance for example – is denied unless	X
	Applicant has implemented host firewall rules that prevent the use of RDP to log into workstations.	
	Applicant has configured all service accounts to deny interactive logons.	X
	None of the above.	
	Additional commentary on segmentation:	
	Bank's reply: Network segmentation is based on geography, business functions and application type **RDP is disabled through configurations settings and not through host firewall rules.**	
19	Enter the date of the **Applicant's** last ransomware exercise; check the box if none has been conducted.	
	Date:	
	No ransomware exercise has been conducted.	X
20	Does the **Applicant** have a documented plan to respond to ransomware of a 3rd party provider/vendor or customer? If yes, please indicate principle steps.	
	No	X
	Yes	
	3rd party ransomware response principle steps:	
21	With regards to verifying the efficacy of security controls, select all that apply to the **Applicant**:	
	Applicant uses Breach and Attack Simulation (BAS) software to verify the effectiveness of security controls.	
	Applicant has an internal "red team" that tests security controls and response.	X
	Applicant has engaged an external party to simulate threat actors and test security controls in the last year.	
	None of the above.	
	Additional commentary on controls verification:	

I.T. Wing, Procurement Group ★ CANARA BANK ★ H.O.

22	With regards to disaster recovery capabilities, select all that apply to the **Applicant:**	
	A process for creating backups exists, but it is undocumented and/or ad hoc	
	Applicant has a documented Disaster Recovery Policy, including standards for backups based on information criticality.	X
	At least twice a year, **Applicant** tests its ability to restore different critical systems and data in a timely fashion from its backups.	
	None of the above.	
23	What is the **Applicant's** Recovery Time Objective (RTO) for critical systems?	
	Applicant does not have an RTO/Does not know	
	< 4 hours.	X
	4-24 hours.	
	1 to 2 days.	
	2-7 days.	
24	With respect to backup capabilities, select all that apply to the **Applicant:**	
	Applicant's backup strategy includes offline backups (can be stored on site)	X
	Applicant's backup strategy includes offline backups stored offsite	X
	Applicant's backups can only be accessed via an authentication mechanism outside of our corporate Active Directory.	X
	Additional commentary on backup capabilities:	
	Bank's Reply: Backups are accessed through TSM solution	
25	Does the **Applicant** have a policy that all portable devices use full disk encryption?	
	Yes	
	No	X
	Additional commentary: NIL	

I.T. Wing, Procurement Group ★ CANARA BANK H.O. Bengaluru - 560 001

Annexure-2

Ransomware Strategy -Q12C

Follow-on question for every service account with Domain Admin privileges:

1) What is the purpose of this service account?
2) Why does this account need domain admin privileges?
3) Footprint where this service account is used? (All endpoints, Workstations only, Servers only or Domain Control only)
4) Type of login permitted for this account (Interactive logon / Network Logon, etc.)
5) Any compensating controls?

12C - Service Account - Data Collection

Username	Purpose	Why is Domain Admin Privilege required?	Footprint of Account. (Used where)	Login permitted for this account (Interactive/ Network / Non-Interactive)	Compensating Controls (if any)	Would Insured be able to remove 'Domain Admin' privilege for account? And by when?
ACCOUNT NAMES (less than 5)	Used in few core applications/services having a high degree of integration with AD	Used in few core applications/services having a high degree of integration with AD	Used at application level only	Non-interactive	Credentials are kept securely	Rights are on a strict need basis, can be removed once the applicability is over

ANNEXURE - 3

Cyber Risk Assessment Questionnaire

Version: MR CRAQUE 2019 LARGE EN V1.DOCX

Print: 17 September 2019

Introduction

This questionnaire is designed to provide us with a comprehensive view of the effectiveness and maturity of information and data security within your company. The answers to the questions are very important to us for assessing the risk in order to provide cyber insurance to you based on the information we receive. Therefore we rely on your statements made in the questionnaire which are the basis for the insurance contract. Considering this, someone within the company responsible for information security should answer and sign the questionnaire or at least support the person who is answering it by countersigning. If you have no information security resource, then the questionnaire should be completed by a senior representative (owner or board member).

This questionnaire is neither an offering nor binding of an insurance contract (coverage). Furthermore the completion of this questionnaire does not obligate the insurer to offer coverage to you.

Are any further information or details regarding your information security enclosed by attachment? ☑ Yes □ No

Currency used for this questionnaire: □ USD □ EUR □ GBP □ Other: ....

1 Company / applicant information

Name of applicant	CANARA BANK
Address	HEAD OFFICE 112, J C ROAD BENGALURU
Country	India
Email	hoditcsg@canarabank.com
Phone	080-25535277
Subsidiaries	
All web domain names that should be covered by this insurance	There are approximately 8 domains like canarabank.com, canarabank.in etc. hosting various underlying sub-domains/applications

1.1 Industrial sector(s)

Please check the industrial sector(s). Details and assignment are available in the annex on page 10.

□ Business & Professional Services

□ Defense / Military Contractor

□ Education

□ Energy

□ Entertainment & Media

□ Information Technology - Software

□ Manufacturing

□ Mining & Primary Industries

□ Pharmaceuticals

□ Public Authority; NGOs; Non-Profit

D.I.T. Wing, Procurement Group
CANARA BANK
H.O., Bengaluru-560 001

☑ Financial Services - Banking

□ Financial Services - Insurance

□ Financial Services - Investment management

□ Food & Agriculture

□ Healthcare

□ Information Technology - Hardware

□ Information Technology - Services

□ Real Estate, Property & Construction

□ Retail

□ Telecommunications

□ Tourism & Hospitality

□ Transportation/Aviation/Aerospace

□ Utilities

□ Other

For "Other" type of industry, please specify	
Please specify details of your activities	

1.2 Turnover/revenue and regional footprint

	Domestic	USA	European Union	Rest of world
Your turnover / revenue for the last fiscal year	84778.19 in Cr INR	100.86 in Cr INR	819.13 in Cr INR	198.97 in Cr INR
Your share of turnover/revenue created online for the last fiscal year	--	--	--	--

	Last year Mar 2022	Year before last -Mar '21	Last but two years -Mar 20
Your gross profit (or equivalent)	23088.98 Cr INR	--	--

Please state the number of employees	85,576 (As on 01.01.2023)
Please state the (estimated) number of individual IT devices deployed	Details cannot be disclosed.

1.3 Type and quantity of data

Please estimate type and volume of the following categories of sensitive data your company is maintaining/processing to the best of your knowledge.

	Type of data	Number of unique records	Number of unique records of	Number of unique records stored in US data centres

I.T. Wing, Procurement Group ★ H.O. Bengaluru-560 001 ★ CANARA BANK

			US citizens	
☑	Personally Identifiable Information (PII)	10,16,39,380		N.A
☑	Payment Card Information (PCI)	Credit card base = 5,93,845 debit card base = 4,97,24,092 (active card)		
□	Protectable Health Information (PHI)			
□	Intellectual property (IP)			

1.4 Requested cyber insurance

Policy period	From	31-03-2023	To	30-03-2022
Aggregate limit requested		As per RFP & per scope document		
Retroactive date		As per RFP & per scope document		
Territorial scope of insurance cover		As per RFP & per scope document		

Cover modules/elements

Please check all cover modules requested. Details and assignment are available in the annex on page 10.

First party losses		Deductible/SIR for each and every insured event	Sub-limit for each and every insured event and in the aggregate
□	Breach and privacy event	As per RFP & per scope document	As per RFP & per scope document
□	Data and software loss		
□	Business interruption		
□	Contingent business interruption		
□	Incident response costs		
□	Regulatory and defence cover		
□	Financial theft and fraud		
□	Cyber extortion		

D.M. Wing, Procurement Group ★ CANARA BANK ★ H.O. Bangalore-560001

Third party claims	Deductible/SIR for each and every insured event	Sub-limit for each and every insured event and in the aggregate
□ Network service failure liability	As per RFP & per scope document	As per RFP & per scope document
□ Technology E&O		
□ Multi-media liability		

1.5 Prior cyber insurance

1 Do you currently hold or have ever held cyber insurance providing the same or similar coverage as the insurance sought? ☑ Yes □ No

2 Has any insurer ever cancelled or non-renewed a policy that provided the same or similar coverage as the insurance applying for? □ Yes ☑ No

1.6 Information Security Events and Loss History

Please answer the following questions by considering any time during the past three years.

1 Have you had any **incidents, claims or suits** involving unauthorized access or misuse of your network, including embezzlement, fraud, theft of proprietary information, breach of personal information, theft or loss of laptops, denial of service, electronic vandalism or sabotage, computer virus or other incident?
☑ Yes □ No **(Please refer to the claim)**

2 Have you experienced an **unplanned business interruption** of longer than four hours caused by a cyber incident? □ Yes ☑No

3 Have you experienced an **extortion attempt or demand** with respect to your computer systems?
□ Yes ☑ No

4 Have you received any **claims or complaints** with respect to allegations of defamation, invasion or injury of privacy, theft of information, breach of information security, transmission of malware, participation in a denial of service attack, request to notify individuals due to an actual or suspected disclosure of personal information? □ Yes ☑No

5 Have you been subject to any **government action, investigation or subpoena** regarding any (alleged) violation of any (privacy) law or regulation? □ Yes ☑ No

6 Are you aware of any **release, loss or disclosure of personally identifiable information** in your care, custody or control, or in the control of anyone holding such information on behalf of you? □ Yes ☑ No

7 Are you aware of any **actual or alleged fact, circumstance, situation, error or omission, or potential issue** which might give rise to a loss or claim against you under the cyber insurance policy for which you are applying for or any similar insurance presently or previously in effect or currently proposed? □ Yes
☑ No

If one question or more of this section 1.6 is answered with "Yes", please attach a description including complete details (cause, costs, notification, time to discover, recovery time and steps taken to mitigate future exposure) of each event (incident, claim etc.).

1.7 Frameworks and Standards

Please check all legal frameworks you have to adhere to.

D.I.T. Wing, Procurement Group
CANARA BANK
H.O. Bengaluru-560 001

☑	General Data Protection Regulation (GDPR) of the European Union (EU) *(Applicable for London Branch)*	□	US Federal Privacy Act
□	US Health Insurance Portability and Accountability Act (HIPAA) and US Health Information Technology for Economic and Clinical Health (HITECH) Act		

Please check all standards for which you have successfully been audited or hold a valid certificate.

☑	Payment Card Industry Data Security Standard (PCI DSS)						
□	Merchant level 1	□	Merchant level 2	☑	Merchant level 3	□	Merchant level 4

□	ISO 27001:2013 Information security management systems	□	NIST (US National Institute of Standards and Technology) Cybersecurity Framework
□	Critical Security Controls	□	Other

□	COBIT 5 (Control Objectives for Information and Related Technologies)	□	Information Security Forum (ISF) The Standard of Good Practice for Information Security 2018

If "Other" standard(s) apply, please specify	
Please describe the scope of the certificate	

Information Security

The following questions help us to evaluate the maturity of your information security. Please answer all questions and provide evidence where available (e.g. reports, presentations, documents etc.). The questions are structured according to the clauses of the ISO/IEC 27002 standard. Hence questions focussing on one security objective can appear in different sections of this questionnaire. In order to create a better understanding about why we ask the questions, each section starts with the objective(s) of the ISO security control categories.

1.8 Information security policies

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

1 Have you developed and implemented a formal information security policy which is corporate-wide and permanently available for all employees and relevant external parties? ☑ Yes □ No

2 Are your information security policies annually reviewed and approved by senior management? ☑ Yes □ No

D.I.T. Wing, Procurement Group ★ H.O., Bengaluru-560 001 ★ CANARA BANK

1.9 Organization of information security

Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.

1 Have you assigned a responsible person for information security (e.g. Chief Information Security Officer "CISO")? ☑Yes □ No

2 Does your IT security responsible person regularly report to senior management? ☑ Yes □ No

3 Do you have an up to date list of authorities and external contacts, which must be informed in case of an information security incident? ☑ Yes □ No

1.10 Human resource security

Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered. To ensure that employees and contractors are aware of and fulfil their information security responsibilities. To protect the organization's interests as part of the process of changing or terminating employment.

1 Do you provide at least annual education to increase your users (employees and contractors) security awareness and to prepare users to be more resilient and vigilant against phishing? ☑ Yes □ No

2 Do you monitor and report to management on security awareness trainings? ☑ Yes □ No

3 Have you identified roles (e.g. privileged users, admins, executives) which need tailored security awareness training? ☑ Yes □ No

1.11 Asset management

Objective: To identify organizational assets and define appropriate protection responsibilities. To ensure that information receives an appropriate level of protection in accordance with its importance to the organization. To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.

1 Do you keep an up-to-date inventory of software (incl. operating systems) and hardware assets in your network? ☑ Yes □ No

2 Do you have a comprehensive Configuration Management Database (CMDB) including: all IT assets, public cloud assets, dependencies, criticality, ownership, software and patch versions? □ Yes ☑ No

3 Do you use a Mobile Device Management (MDM) solution for all laptops and smartphones? ☑Yes □ No

4 Do you classify information with regards to confidentiality? ☑ Yes □ No

5 Do you classify information with regards to integrity and availability requirements? ☑ Yes □ No

6 Are Information labelling procedures implemented in accordance with the above classification scheme? ☑Yes □ No

7 Have you technically enforced the information classification scheme? □ Yes ☑ No

8 Do you provide guidance how to handle classified information? ☑ Yes □ No

9 Is the handling of information reviewed on a regular basis in order to ensure consistency with its classification? ☑ Yes □ No

D.I.T. Wing, Procurement Group ★ CANARA BANK ★ H.O. Bengaluru-560 001

10 Do you either restrict access to or encrypt confidential information stored on removable media like external storage devices (e.g. USB sticks or hard disks)? ☑ Yes □ No

11 Is an authorization required for media removed from the organization and is a record of such removals kept in order to maintain an audit trail? ☑ Yes □ No

12 Are media ports (e.g. USB) managed centrally or generally deactivated? ☑ Yes □ No

13 Do you securely dispose media containing sensitive information if it is not used any longer? ☑ Yes □ No

14 Do you enforce guidelines that the content - if no longer required - of any re-usable media that can be removed from the organization are made unrecoverable? ☑ Yes □ No

1.12 Access control

Objective: To limit access to information and information processing facilities. To ensure authorized user access and to prevent unauthorized access to systems and services. To make users accountable for safeguarding their authentication information. To prevent unauthorized access to systems and applications.

1 Do you restrict employees' and external users' privileges on a business-need to know basis (particularly administrative permissions and access to sensitive data e.g. personal data)? ☑ Yes □ No

2 Have you enforced multi-factor authentication for remote access? ☑Yes □ No □ Not applicable

3 Do you have a formal access provisioning process in place for assigning and revoking access rights? ☑ Yes □ No

4 Do you have implemented a central Identity and Access Management ("IAM") system for assigning and revoking access rights? ☑ Yes □ No

5 Does the data owner at least annually review access rights? ☑ Yes □ No

6 Do you prohibit local admin rights on workstations for users? ☑ Yes □ No

7 Do you use Privileged Identity and Account Management ("PIM", "PAM")? ☑ Yes □ No

8 Do you review user access rights at least annually? ☑ Yes □ No

9 Do you review shared accounts (e.g. used for high-privileged systems/applications) at least annually? ☑ Not applicable □ Yes □ No

10 Do you review authorizations for privileged access rights intervalic at least on a bi-annual basis? ☑ Yes □ No

11 Do you revoke all system access, accounts and associated rights after termination of users (incl. employees, temporary employees, contractors or vendors)? ☑ Yes □ No

12 Do you have a process to remove unneeded user rights after organizational role changes? ☑ Yes □ No

13 Have you implemented a password policy enforcing the use of long and complex passwords across your organisation? Long and complex passwords are defined as: eight characters or more; not consisting of words included in dictionaries; free of consecutive identical, all-numeric or all-alphabetic characters. ☑ Yes □ No

14 Have you changed all default passwords on all your connected devices (e.g. router, Internet of Things)? ☑ Yes □ No

15 Do you provide an approved password manager for all your users? □ Yes ☑ No

D.I.T. Wing, Procurement Group ★ CANARA BANK ★ H.O. Bengaluru-560 001

1.13 Cryptography

Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

1 Is all confidential information stored on mobile devices (e.g. smart phones and laptops) encrypted?

☑ Yes □ No

(MDM is installed for bank issued laptops which are allowed to connect Bank's network)

2 Do you encrypt sensitive data and confidential information that is stored in databases and file servers? ☑ Yes □ No

3 Have you developed and implemented a policy on the use, protection and lifetime of cryptographic keys? ☑ Yes □ No (As part of IS Policy)

4 Is your policy on cryptographic keys regularly reviewed and updated through their whole lifecycle?

☑ Yes □ No (As part of IS Policy)

1.14 Physical and environmental security

Objective: To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities. To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.

1 Do you maintain a list of personnel (employees, vendors and visitors) with authorized access to your premises and sensitive security areas? ☑ Yes □ No

2 Have you installed advanced entry controls (e.g. biometric access control, mantraps)? ☑ Yes □ No

3 Have you installed advanced entry monitoring controls (e.g. 24-7 closed circuit television (CCTV), documentation of every access)? ☑ Yes □ No

1.15 Operations security

Objective: To ensure correct and secure operations of information processing facilities. To ensure that information and information processing facilities are protected against malware. To protect against loss of data. To record events and generate evidence. To ensure the integrity of operational systems. To prevent exploitation of technical vulnerabilities. To minimise the impact of audit activities on operational systems.

1 Have you implemented change management procedures for critical systems? ☑ Yes □ No

2 Do your change management processes include testing, failback scenarios and reporting? ☑ Yes □ No

3 Does your decision to change the IT environment always consider requirements of business processes?

☑ Yes □ No

4 Is the IT-environment for development and testing separated from production IT-environment?

☑ Yes □ No □ Not applicable

5 Do your developers use different accounts for development, testing and day- to-day tasks?

☑ Yes □ No □ Not applicable

6 Do you use malware protection for all web-proxies, email-gateways, workstations and laptops? ☑ Yes □ No

7 Are updates of anti-malware signature files downloaded and installed automatically? ☑ Yes □ No

8 Besides traditional signature-based detection, does your malware protection use advanced heuristic- and behavioural-based detection mechanisms to protect against new malware? ☑ Yes □ No

9 Do you perform at least weekly regular backups of business critical data? ☑ Yes □ No

10 Do you store backups physically separated from your network (e.g. outside the office premises)? ☑ Yes □ No

11 Do you regularly ensure that data backups are complete and can be restored as quickly as possible with minimal impact to business? ☑ Yes □ No

12 Do you produce and regularly review event logs recording user activities, exceptions, faults and information security events (at least from your firewalls and domain controller)? ☑ Yes □ No

13 Do you have a Security Information and Event Management (SIEM) system in place including rules for generating reports and alerts on system security? ☑ Yes □ No

14 Have you implemented a centralized software installation process? ☑ Yes □ No

15 Do you apply a strict configuration management approach and develop secure images that are used to build all newly deployed workstations and servers? ☑ Yes □ No
(Workstations:Yes, Servers:The hardened image is applicable for VMs only)

16 Do you timely - at least within one month of release - apply updates to critical IT-systems and applications ("security patching")? ☑ Yes □ No

17 Do you timely - at least within one week of release - install security patches on internet-facing IT-systems and applications? ☑ Yes □ No

(Regular patches are being applied on N-1 basis which is in tune with industry best practices and critical/high risk patches are deployed immediately. For Servers, we use Virtual Patching method also to mitigate the Zero-day vulnerabilities.)

18 Do you regularly perform vulnerability scans, identify the associated risk and take appropriate actions? ☑Yes □ No

19 Do you technically or organisationally ensure that users must not install software on their workstations by themselves? ☑ Yes □ No

1.16 Communications security

Objective: To ensure the protection of information in networks and its supporting information processing facilities. To maintain the security of information transferred within an organization and with any external entity.

1 Are all internet access points secured by appropriately configured firewalls? □ Yes □ No
(Not applicable. Bank doesn't use Internet Access Points. Bank has corporate proxy solution for secure internet access.)

2 Are all internet access points secured by Next-Generation Firewalls? ☑ Yes □ No

3 Have you implemented a Network Access Control ("NAC") technology to access your corporate wireless networks? ☑ Yes □ No

4 Do you monitor your network and identify security events? ☑ Yes □ No

5 Are you using an Intrusion Detection System (IDS)? ☑ Yes □ No

6 Do you have a Security Operations Centre (SOC) monitoring all events on a 24-7 basis? ☑ Yes □ No

7 Are all internet-accessible systems (e.g. web-, email-servers) segregated from your trusted network (e.g. within a demilitarized zone (DMZ) or at a 3rd party provider)? ☑ Yes □ No □ Not applicable

G.I.T. Wing, Procurement Group ★ H.O. Bengaluru-560 001 ★ CANARA BANK

8 Are all high risk network segments (e.g. point of sales (PoS) systems, sensitive data processing, office and operational technology (OT) production networks etc.) segregated? ☑ Yes ☐ No ☐ Not applicable

9 Do you encrypt confidential communication (e.g. secure emails with SMIME (Secure Multipurpose Internet Mail Extensions) or SMTP-over-TLS (Simple Mail Transfer Protocol Secure))? ☑ Yes ☐ No

10 Do you use data loss prevention (DLP) software? ☑ Yes ☐ No

1.17 System acquisition, development and maintenance

Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks. To ensure that information security is designed and implemented within the development lifecycle of information systems. To ensure the protection of data used for testing.

1 Does your web-server encrypt confidential data (e.g. HTTPS)? ☑ Yes ☐ No ☐ Not applicable

2 Do you protect your web-servers against denial of service attacks (e.g. by No utilising a content delivery network provider)? ☑ Yes ☐No ☐ Not applicable

3 Do you test security functionality during the development lifecycle of information systems incl. IT security updates? ☑ Yes ☐ No ☐ Not applicable

4 Do you conduct automated security tests or code analysis during system development? ☐ Yes ☑ No ☐ Not applicable

5 Do you consider confidentiality when using operational data for testing to ensure that all sensitive details are protected by removal or modification? ☑ Yes ☐ No ☐ Not applicable

1.18 Supplier relationships

Objective: To ensure protection of the organization's assets that is accessible by suppliers. To maintain an agreed level of information security and service delivery in line with supplier agreements.

1 Have you identified and documented all your important suppliers (including third party service providers)? ☑ Yes ☐ No

2 Have you identified and mandated information security controls to specifically address supplier access to your information in a policy? ☑ Yes ☐ No

3 Do agreements with third party service providers require levels of security commensurate with your own information security standard? ☑ Yes ☐ No

4 Do you periodically review and update agreements with your important suppliers (including third party service providers)? ☑ Yes ☐ No

5 Do you stipulate the right for third party audits within your contractual agreements? ☑ Yes ☐ No

6 Do you monitor third party service provider activities for security events to maintain an agreed level of information security? ☑ Yes ☐ No

7 Do you conduct audits (information security assessments) of suppliers (including third party service providers) and follow-up on issues identified? ☑ Yes ☐ No

8 Do your written and signed contracts with suppliers (including third party service provider) include a hold harmless agreement or waiver of liability in your favour in case such suppliers fail to safeguard your sensitive data? ☑ Yes ☐ No

1.19 Information security incident management

Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

1 Do you have an information security incident response plan in place? ☑ Yes □ No

2 Have you appointed a responsible person or team for incident response? ☑ Yes □ No

3 Do you annually test your security incident response plan? ☑ Yes □ No
(Through table top exercises and drills)

4 Do all your employees and third party providers know the reporting line for information security events?
☑ Yes □ No

5 Are all employees and contractors aware of their responsibility to report information security events?
☑ Yes □ No

6 Do you document all information security events in a central Security Information and Event Management (SIEM) system? ☑Yes □ No

7 Are employees and contractors required to report any identified information security weakness (not yet an incident or event) in systems or services? ☑ Yes □ No

8 Do you offer a bug bounty program for reporting bugs, exploits or vulnerabilities? □ Yes ☑ No

9 Have you established an escalation procedure for information security incidents? ☑ Yes □ No

10 Do you collect evidence for forensic analysis? ☑ Yes □ No

11 Do you regularly inform management about past incidents? ☑ Yes □ No

12 Do you use knowledge gained from analysing and resolving information security incidents to reduce the likelihood or impact of future incidents? ☑ Yes □ No

13 Do you quantify and monitor types, volumes and costs of information security incidents? ☑ Yes □ No

1.20 Information security aspects of business continuity management

Objective: Information security continuity should be embedded in the organization's business continuity management systems. To ensure availability of information processing facilities.

1 Have you conducted a Business Impact Analysis (BIA)? ☑ Yes □ No

2 Are Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for critical systems and processes defined and documented? ☑ Yes □ No

3 Do you have a Business Continuity Management (BCM) plan in place that specifically addresses cyber incidents?
☑ Yes □ No
(Bank has Cyber crisis management plan)

4 Do you have an IT Disaster Recovery (DR) plan in place? ☑ Yes □ No

5 Do you have advanced implementation controls for disaster recovery capabilities in place (e.g. full redundancy or automatic failover mechanisms)? ☑ Yes □ No

6 Do you test your information security continuity plans (e.g. Business Continuity Management, Disaster Recovery) at least annually? ☑ Yes □ No

7 Do you review and update your information security continuity plans (e.g. Business Continuity Management, Disaster Recovery) plans at least annually? ☑ Yes □ No

8 Are the results of the continuity test activities reviewed, documented, reported to management and are the plans revised based on lessons learned? ☑ Yes □ No

9 Are your information processing facilities (i.e. any system, service or infrastructure, or physical location housing it) implemented with redundancy? ☑ Yes □ No

10 Do you regularly - at least annually - conduct redundancy testing to ensure the failover from one component to another component works as intended? ☑ Yes □ No

1.21 Compliance

Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements. To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.

1 Have you implemented a procedure to permanently comply with all privacy relevant legislative statutory, regulatory and contractual requirements? ☑ Yes □ No
(As applicable for relevant jurisdictions)

2 Have you assigned a Compliance Officer? ☑ Yes □ No

3 Does your Compliance Officer regularly report to senior management? ☑ Yes □ No

4 Do you have guideline issued on the retention, storage, handling and disposal of records and information? ☑ Yes □ No

5 Do you have a documented retention schedule to identify records and the period of time for which they should be retained? ☑ Yes □ No

6 Have you assigned a responsible person for providing guidance and ensuring awareness of privacy principles (e.g. Data Privacy Officer DPO)? □ Yes ☑ No

7 Does your Privacy Officer regularly report to senior management? ☑Not applicable □ Yes □ No

8 Do you have a policy for the privacy and protection of personally identifiable information developed and implemented? ☑ Yes □ No (Bank does not have an exclusive Data protection policy. However, few Data protection requirements as per IT Amendment Act 2008 & Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules 2011 (IT RSPPSPI Rules) are mentioned as part of Information Security Policy. For Foreign branches, Bank is having separate policies in compliance with host country regulations.

9 Do you regularly scan critical systems (incl. penetration tests or vulnerability assessments) - either by yourself or supported by third party - particularly each time new systems are introduced and following changes? ☑ Yes □ No

2 Additional Comments and Signature(s)

Would you like to share further information or details regarding your information security?

NIL

D.I.T. Wing, Procurement Group ★ H.O., Bengaluru-560001 CANARA BANK

Annex 1: Overview - Industrial sectors

Source: Cyber Insurance exposure data schema v1.0 by Cambridge Centre for Risk Studies

Business & Professional Services	Occupations providing specialist business advice and services. Some professional services require holding professional licenses such as architects, auditors, engineers, doctors and lawyers.
Defense / Military Contractor	Defense industry comprises government and commercial industry involved in research, development, production, and service of military materiel, equipment and facilities
Education	Colleges and universities, independent and unified school districts, student loans and tuition companies
Energy	Companies involved in the exploration, extraction and development of oil or gas reserves, oil and gas drilling, or integrated power firms.
Entertainment & Media	Enterprises involved in providing news, information, and entertainment: radio, television, films, theatre
Financial Services - Banking	Companies engaged in commercial banking, savings institutions, credit unions, credit card issuing, sales financing, mortgage and loan companies and brokers, financial transaction processing, reserve and clearinghouse activities, and central banking.
Financial Services - Insurance	Direct insurance carriers, reinsurance carriers, and insurance agencies and brokerages.
Financial Services - Investment management	Companies engaged in investment banking, securities dealing and brokerage, commodity contracts dealing and brokerage, securities and commodity exchanges, investment clubs and venture capital, portfolio management, investment advice, and legal entity funds and trusts
Food & Agriculture	Those involved in the food industry, including production, processing, distribution, and wholesale supply
Healthcare	Companies providing goods and services to treat patients with curative, preventive, rehabilitative, and palliative care.
Information Technology - Hardware	Companies engaged in manufacturing and/or assembling computers (mainframes, personal computers, workstations, laptops, and computer servers) and peripheral equipment (e.g. storage devices, printers, monitors etc.)
Information Technology - Services	Companies providing hosting or data processing services (incl. cloud and streaming services); internet publishing and broadcasting content (incl. social media); internet search portals; services relating to computer systems design, computer facilities management, computer programming services, and computer hardware or software consulting.
Information Technology - Software	Companies involved in the design, development, documentation, and publishing of computer software
Manufacturing	Companies making or process goods, especially in large quantities and by means of industrial machines
Mining & Primary Industries	Companies involved in the mining, quarrying, and processing of extracting minerals, coal, ores, main commodities, and natural resources.
Pharmaceuticals	Pharmaceutical industry develops, produces, and markets drugs or pharmaceuticals for use as medications. Pharmaceutical companies may deal in generic or brand medications and medical devices.

Public Authority; NGOs; Non-Profit	National or local government agencies, non-governmental and non-profit organizations
Real Estate, Property & Construction	Companies managing, developing, and transacting property consisting of land and buildings, along with its natural resources such as crops, minerals, or water
Retail	Retailers to general public, sellers of goods and services both in retail stores and online, wholesalers and distributors.
Telecommunications	Companies facilitating exchange of information over significant distances by electronic means.
Tourism & Hospitality	Companies providing services for tourism, travel, accommodation, catering and hospitality
Transportation/ Aviation/ Aerospace	Companies facilitating the transportation of goods or customers. The transportation sector is made up of airlines, railroads and trucking companies.
Utilities	The utilities sector contains companies such as electric, gas and water firms and integrated providers

Annex 2: Overview - Coverage modules/elements

Breach and privacy event	The cost of responding to an event involving the release of information that causes a privacy breach, including notification, compensation, credit-watch services and other third party liabilities to affected data subjects, IT forensics, external services, and internal response costs, legal costs.
Data and software loss	The cost of reconstituting data or software that have been deleted or corrupted.
Business interruption	Lost profits or extra expenses incurred due to the unavailability of IT systems or data as a results of cyber attacks or other non-malicious IT failures.
Contingent business interruption	Business interruption resulting from the IT failure of a third party, such as a supplier, critical vendor, utility, or external IT services provider.
Incident response costs	Direct costs incurred to investigate and close the incident to minimise post-incident losses. Applies to all the other categories/events.
Regulatory and defence coverage	Covers the legal, technical or forensic services necessary to assist the policyholder in responding to governmental inquiries relating to a cyber attack, and provides coverage for fines, penalties, defence costs, investigations or other regulatory actions where in violation of privacy law; and other costs of compliance with regulators and industry associations. Insurance recoveries are provided where it is permissible to do so.
Financial theft and fraud	The direct financial loss suffered by an organisation arising from the use of computers to commit fraud or theft of money, securities, or other property.
Cyber extortion	The cost of expert handling for an extortion incident, combined with the amount of the ransom payment.
Network service failure liability	Third-party liabilities arising from security events occurring within the organisation's IT network or passing through it in order to attack a third-party.
Technology E&O	Coverage for third party claims relating to failure to provide adequate technical service or technical products including legal costs and expenses of allegations resulting from a cyber attack or IT failure.

Multi-media liability	Cost for investigation, defence cost and civil damages arising from defamation, libel, slander, copyright / trademark infringement, negligence in publication of any content in electronic or print media, as well as infringement of the intellectual property of a third party.

D.I.T. Wing, Procurement Group ★ CANARA BANK ★ H.O., Bengaluru - 560 001

ANNEXURE - 4

Note on Claim Reported under the Cyber Insurance Policy of Canara Bank issued by The New India Assurance Company Limited Policy Period : 31st March 2020 to 30th March 2021

- A Cyber Fraud was intimated by the Bank in the month of March 2021.Access to LAN cable of ATMs were gained by fraudsters via spoofing. The messages of transactions declined by ATM Switch have been altered to successful transactions to make the ATM machines dispense cash.
- The loss amount from all affected ATMs is INR 72.75 lacs.
- The deductible under the Policy is INR 50 lacs.
- The claim is likely to fall within the deductible in light of the recovery effected.