Pre Bid Queries Replies of RFP 29/2020-21 dated 28/01/2021 for Selection of Insurer for Renewal of Cyber Risk Insurance Policy for Canara Bank from 31st March 2021 to 30th March 2022

Sl. No.	Clause No.	Page No.	Clause	Bidder's Query	Bank's Reply
1	NA	NA	NA	Kindly provide IT security Policy	Policy documents are internal & confidential in nature. It will be shared to selected bidder.
2	NA	NA	NA	Kindly provide Business Continuity Plan or kindly revert to points as requested to be answered in below table, alternatively. (table seperately attached)	BCP documents are internal & confidential in nature. It will be shared to selected bidder.
3	NA	NA	NA	Please provide comments on the exposure of total number of Proprietary & Confidential data that the organization host, store, share, transmit, publish, or transact. ▫ Total number of Credit Card / Debit Card Information ▫ Total number of other personally identifiable information such AADHAR Card number, Driving Licence etc	No Comments Proprietary & Confidential data of the organization are confidential in nature & will be shared only to selected bidder after entering NDA Total No. of Debit cards - 3.88 Crores Total No. of Credit Cards - 2.85 Crores Total no. of Customers KYC complied - 7.21 Crores (information like aadhar, PAN, Passport, DL, Voter ID etc. submitted)
4	NA	NA	NA	Please provide comments on the exposure of published electronic content	It is available in www.canarabank.com
5	NA	NA	NA	Does the organization's data protection policy comply with the data protection and privacy legislation applicable to all jurisdictions and industry standards/requirements, in which the organization operates?	YES, For overseas Branches it is there. For Indian Branches the legislation is yet to be made.Bank's data protection policy is part of Information Security Policy.
6	NA	NA	NA	Has the Security Incident Response Plan been reviewed and approved by the organization's Board of Directors or persons with substantially similar responsibilities?	YES
7	NA	NA	NA	Does the organization subscribe to any Dark & Deep Web Monitoring Services, which gives visibility to sensitive information disclosure, breached data, and leaked credentials?	YES
8	NA	NA	NA	Does the organization conduct external Red Teaming or Opportunistic Hacking exercises in every financial year?	YES
9	NA	NA	NA	Does the organization take cybersecurity initiatives for spreading information security awareness through emailers, posters, banners, tabletop cards, or desktop screensavers to employees at least twice in a year?	YES
10	NA	NA	NA	Does the organization review, update, and test the Disaster Recovery (DR) plan in every financial year?	YES

Sl. No.	Clause No.	Page No.	Clause	Bidder's Query	Bank's Reply
11	NA	NA	NA	Does the organization have an information classification scheme based on information confidentiality, integrity, and availability?	YES
12	NA	NA	NA	Does the organization secure physical access to organization facilities (e.g., offices, data centres), equipment (e.g., servers, workstations), and storage media (e.g., removable media, paper records), which contain sensitive information?	YES
13	NA	NA	NA	Does the organization harden all servers and workstations, e.g., removing unnecessary software, logins, services that are not required to fulfil the intended task by the program?	YES
14	NA	NA	NA	Does the organization have any wireless networks, either open (unencrypted) or secured using the WEP encryption standard?	Bank does not provide Corporate Network in Wireless mode. Bank has wireless networks & is totally encrypted.
15	NA	NA	NA	Does the organization use an Integrated Risk management platform?	BANK has Enterprise Wide Integrated Risk Management Solution in Place.
16	NA	NA	NA	Does the organization have two-factor authentication implemented for email, application authentication, cloud services access, and remote access?	email - Not available Customer application - Dual authentication Cloud services access - Covered above Remote access - Yes
17	NA	NA	NA	Does the organization have a Load Balancer in place to maintain the availability of critical resources?	YES
18	NA	NA	NA	Does the organization have a Network Access Control (NAC) solution in place?	YES
19	NA	NA	NA	Does the organization have an Incident/Change tracking solution in place?	YES - CMR Package, Incident Management package
20	NA	NA	NA	Does the organization have a Security Incident and Event Management (SIEM) solution in place?	YES
21	NA	NA	NA	Does the organization have an Identity & Access Management (IAM) solution in place?	YES (Active Directry for end points, SAS applications, PIM servers & DAM database)
22	NA	NA	NA	Does the organization have a Mobile Device Management (MDM) solution in place?	YES
23	NA	NA	NA	Does the organization have a Database Activity Monitoring (DAM) solution in place?	YES
24	NA	NA	NA	Does the organization have Deception Tools & Honeypots in place?	YES

Sl. No.	Clause No.	Page No.	Clause	Bidder's Query	Bank's Reply
25	NA	NA	NA	Does the organization have a Security Operations Analytics and Reporting (SOAR) solution in place?	NO. The same is in Process for implementing in future
26	NA	NA	NA	Does the organization have a User and Entity Behaviour Analytics (UEBA) solution in place?	NO. The same is comparable with Banks existing Anti-APT Solution
27	NA	NA	NA	Does the organization have a Web Application Firewall (WAF) in place?	YES
28	NA	NA	NA	Does the organization have a Next Generation Firewall (NGFW) or Unified Threat Management (UTM) solution in place, which is capable of intrusion detection and prevention?	YES
29	NA	NA	NA	Does the organization have an Advanced Persistent Threat (APT) solution in place?	YES
30	NA	NA	NA	Does the organization have a Zero-Day Detection solution in place?	Yes.Bank has ANTI-APT Solution.
31	1 & 5	Proposal form	Data protection procedure, question a & Other information question d	Please share information security policy, RTO in case of IT infra failure	Policy documents are internal & confidential in nature. It will be shared to selected bidder. RTO in case of IT infra failure is doccumented as per industry standards. (ie., 2 hours)
32	4	Cyber maturity assessment questionnaire	Question no 9	What is the frequency of validation of log reports to uncover the anomalies of Critical System Components? For how long logs are stored?	YES, SOC is Present
33	3	Proposal form	Data access and recovery question a	How often assessment programs run to determine whether all systems' software's & security patches are updated?(including remote access connection)	YES, for all endpoints as per the Bank's Policy.
34	4	Proposal form	Data access and recovery question i	How many times data restoration process is verified to ensure back up data is properly working? Is backed up data encrypted?	Monthly
35	4	Proposal form	Outsourcing activities question a	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?	Only one outsourced Vendor is present & it's as per the Bank's Outsourcing Policy
36	3	Proposal form	Data access and recovery question d	How often all the Ports are scanned against all critical servers for to & fro data movement ? Is SOC empowered to perform continuous data monitoring?	Daily Scanning of ports. SOC Implemented

Sl. No.	Clause No.	Page No.	Clause	Bidder's Query	Bank's Reply
37	3	Proposal form	Data access and recovery question c	Does the company have checks in place to identify and detect network security weakness? (internal/External Vulnerability assessment)	YES, VAPT in place
38	3	Proposal form	Data access and recovery question b	Does company have Anti virus & Firewall installed on computer system? If yes, What is the frequency for updating this? Which EDR solution is installed on all end points?	YES, we have Anti-APT.
39	3	Proposal form	Data access and recovery question h	Is data in stored form(On Cloud, Servers, Laptops, Flash drives, back up tapes) or in transit form, encrypted using strong encryption technologies? Which encryption technologies are used?	YES, Data is encrypted in REST & TRANSIT
40	3	Proposal form	Data access and recovery question e	How many times Admin access rights are reviewed to ensure only that only administrative functions (Non-Internet Connection based) are performed on those systems?	Concurrent Audit done Monthly & Quarterly for Both DC & DRC.
41	3	Proposal form	Data access and recovery question e	In case of cyber attack, which multilayer boundary defence are in place to filter inbound and outbound traffic(including business partner network)?	Defence in depth approach is followed with multiple solutions.
42	3	Proposal form	Data access and recovery question c	Is comparison of firewall, router and switch configuration against standard for each network devices performed?	YES, Hardening & Configuration audit is performed.
43	3	Proposal form	Data access and recovery question c	Is cyber security assessment performed for all applications before moving into production?	YES
44	3	Proposal form	Data access and recovery question e	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
45	3	Proposal form	Data access and recovery question g	Is financial messaging systems (NIFT/SWIFT) is audited regularly?	YES
46	6	Proposal form	Claim Information, proposal form mention only claims not incidences	Mention any cyber incidents (Success/Failed) happened in past with organization?	No such incidents reported.
47	NA	NA	NA	Latest IT and Cyber Security policy copy	Policy documents are internal & confidential in nature. It will be shared to selected bidder.

Pre Bid Queries Replies of RFP 29/2020-21 dated 28/01/2021 for Selection of Insurer for Renewal of Cyber Risk Insurance Policy for Canara Bank from 31st March 2021 to 30th March 2022

Sl. No.	Clause No.	Page No.	Clause	Bidder's Query	Bank's Reply
48	NA	NA	NA	Business Continuity plan (BCP) and Disaster recovery plan (DRP) copy	Policy documents are internal & confidential in nature. It will be shared to selected bidder.
49	NA	NA	NA	Network security policy copy - Latest	Policy documents are internal & confidential in nature. It will be shared to selected bidder.
50	NA	NA	NA	Password Management/Protection policy copy	Policy documents are internal & confidential in nature. It will be shared to selected bidder.
51	NA	NA	NA	Any Claims has been reported ?	No claims reported
52	NA	NA	NA	What the latest IT security measures being taken by the M/s Canara Bank -	IT security measures being taken by the M/s Canara Bank is a confidential information & will be shared to selected bidder only under NDA. SOC is implemented, CISO is nominated by Bank, Application audit is conducted & Security Audit done.
53	NA	NA	NA	Has the Company been the subject of any investigation or audit in relation to data protection by a Data Protection Authority or other regulator?	NO
54	NA	NA	NA	Has the Company ever been subject to a Data Subject Access Request?	NO
55	NA	NA	NA	Is the Company after due inquiry aware of any actual or alleged fact or circumstance which may give rise to a claim under this policy?	NO
56	NA	NA	NA	Duly Filled Proposal form (It was provided in last year tender process)	Already Shared
57	NA	NA	NA	Premium under the expiring policy	Premium cannot be shared
58	Annexure 5	37	Scope of Work	Expiring Policy Copy with terms & Conditions, Policy limits, covers & Deductibles	As per the RFP Scope covered.
59	Annexure 5	37	Scope of Work	Placement structure of expiring policy (any coinssurance) considering the SumInsured limit of 370Cr	Refer Scope Document
60	Annexure 5	37	Scope of Work	Last 3 years claims experience/notifications if any	No claims reported in last 3 years
61	Annexure 5	37	Scope of Work	Whether Insured's BI Policy has Cyber Crime extension, if yes limits opted therein	Refer Scope Document
62	NA	NA	NA	Policy copy along-with expiring premium.	Cannot be Shared
63	NA	NA	NA	Claim history and incident history for last 3 years.	No Claim till date
64	NA	NA	NA	IT security plan/business continuity plan/disaster recovery plan.	The subject Documents are internal & confidential in nature. It will be shared to selected bidder.

Sl. No.	Clause No.	Page No.	Clause	Bidder's Query	Bank's Reply
65	NA	NA	NA	IT audit report.	It is the Bank's confidential document & cannot be disclosed.
66	NA	NA	NA	BITSIGHT or any other similar credit rating report.	No such Credit rating report. However Bank's IT department is ISO 270001/2013 certified.
67	NA	NA	NA	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
68	NA	NA	NA	Does the organization conduct simulated phishing campaigns every financial year, targeting business-sensitive employees within the organization and subsequently provide training for preparing employees to be more resilient and vigilant against phishing attacks?	Yes
69	NA	NA	NA	Does the organization conduct domain-related security training tailored to specific roles for all employees (including senior management) in every financial year to ensure all employees are implementing effective cybersecurity concepts in their specific domain?	Yes
70	NA	NA	NA	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
71	NA	NA	NA	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
72	NA	NA	NA	Does the Applicant have a documented process to respond to phishing campaigns (whether targeted specifically at the Applicant or not)?	Yes
73	NA	NA	NA	Steps taken by the company to prevent potential Data Breach incidents due to all/most employees working from home?	Bank has Work From Home Policy & provision made only to selective staff only. Secure solution is provided. Direct access not provided to Servers/Critical resources.
74	NA	NA	NA	Is there a BCP plan in place? Has the BCP been tested for a scenario where all/most employees must work either from home or alternate locations? Has the insured discussed their BCP with their regulators, and if yes what has been the response?	YES / NO / YES Observations of RBI have been attended / are being attended.

Sl. No.	Clause No.	Page No.	Clause	Bidder's Query	Bank's Reply
75	NA	NA	NA	Did the IT infrastructure function as normal because of the lockdown? If not, please provide details of areas not at full functionality. How is severity	YES
76	NA	NA	NA	Under the BCP operating environment is it possible to maintain standard risk/operational controls and procedures? If not, please provide full details of all weaknesses and/or any reduction in the control environment, as well as the impact this has to the insured's operational resilience.	YES, standard risk/operational controls and procedures are in place
77	NA	NA	NA	What plans has the company put in place to mitigate any IT or control weaknesses? Please confirm that all necessary IT security measures including VPN, MFA etc. are implemented for the remote connections.	Risk assesment is being Done & Risk register is put up to the Board.
78	NA	NA	NA	Has the regulator imposed any restrictions on the insured whilst operating under their alternative operating environment pursuant to their BCP?	NO such instances
79	NA	NA	NA	Do you have log monitoring?	YES

Date: 08/02/2021
Place: Bengaluru

Deputy General Manager