Replies to Prebid Queries for GEM/2022/B/1853849 dated 12/01/2022 for selection of insurer for renewal of cyber risk insurance policy for Canara Bank from 31st march 2022 to 30th march 2023

Sl.No.	GeM bid clause	Clause/ Requirement	Bidder Query	Bank's Reply
1	NA	NA	Does the company have Board approved Information Security & privacy policy and it is communicated to all stakeholders?	Yes
2	NA	NA	Does the company have Board approved Incident Response Plan, Disaster recovery plan, Business Continuity plan and are they reviewed at least annually?	Yes
3	NA	NA	Mention the duration in which the company likely to incur a loss of profit after a cyber-attack?	Details will be shared with the selected bidder
4	NA	NA	Has your organization been compromised in past?	No
5	NA	NA	Which are the information security certification hold by your organization?	ISO/IEC 27001:2013 Certified
6	NA	NA	What is the impact/severity in terms of daily loss of profit after cyber attack or interruption in company's IT network?	As per BIA
7	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?	Yes
8	NA	NA	Does it require to comply with data protection laws applicable to jurisdictions in which company operates?	Yes
9	NA	NA	Has organization been ever investigated in relation to safeguard of personal information?	Not arised
10	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)	Bank is conducting various trainings. However, the count will be informed to selected bidder.
11	NA	NA	Are security audit logs generated for all hardware and softwares installed on it?	Yes
12	NA	NA	What is the frequency of validation of log reports to uncover the anomalies of Critical System Components?	SIEM is in place
13	NA	NA	Are only fully supported/updated web browsers and email clients allowed to execute in the organization?	Yes
14	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
15	NA	NA	How often assessment programs run to determine wheather all systems' softwares & security patches are updated?(including remote access connection)	Monthly
16	NA	NA	Does company have Anti-virus & Firewall installed on computer system? If yes, What is the frequency for updating this?	Yes, as and when OEM released
17	NA	NA	Is comparision of firewall, router and switch configuration against standard for each network devices performed?	Yes
18	NA	NA	Is cyber security assessment performed for all applications before moving into production?	Yes
19	NA	NA	Is any network access control technology in place to authorize authenticated devices and software installation before allowing them on the network?	Yes
20	NA	NA	How often all the Ports are scanned against all critical servers for to & fro data movement?	Regularly
21	NA	NA	Does the company have checks in place to identify and detect network security weakness? (internal/External Vulnerability assessment)	Yes, through Internal & External Vulnerability Assessment
22	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	Yes, Internal every Six month & external annually
23	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	Multiple Firewall are in place to filter inbound & outbound traffic (including business partner network)
24	NA	NA	Which type of data organization collect, store & process? (Multiple Choice)	Only Customer Account specific
25	NA	NA	What is the frequency of Data Back Up(Operating System, Application Software and Data)?	Data Backup Process is in place as per Bank's policy
26	NA	NA	How many times data restoration process is verified to ensure back up data is properly working?	Data Restoration Process is verified to ensure backup data as per Bank's Policy

D.I.T. Wing, Procurement Group, CAN[illegible] Bengaluru-560 0[illegible]

Replies to Prebid Queries for GEM/2022/B/1853849 dated 12/01/2022 for selection of insurer for renewal of cyber risk insurance policy for Canara Bank from 31st march 2022 to 30th march 2023

Sl.No.	GeM bid clause	Clause/ Requirement	Bidder Query	Bank's Reply
27	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?	Data in transit and Data at rest is encrypted
28	NA	NA	Are data access restrictions inforced on the basis of specific role rights ?	Yes
29	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?	Monthly
30	NA	NA	Which user access management methods are being used in your organization?	Active Directory
31	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?	Previlege Identity Management is in place
32	NA	NA	Please share information security policy, RTO in case of IT infra failure	Details will be shared with the selected bidder
33	NA	NA	Is SOC empowered to perform continuous data monitoring?	No
34	NA	NA	Which EDR solution is installed on all end points?	No
35	NA	NA	Is financial messaging systems (NIFT/SWIFT) is audited regularly?	Yes
36	NA	NA	Please share claim details under existing Cyber Policy ending on 30th March 2022	NIL.
37	NA	NA	Please confirm Current status of claim along with Admissibility status along with Claim Reserve Created by Insurer	Currently, the claim is under process with the insurer and insurer has created reserves for Rs.22.75 Lakhs and final survey report is awaited.
38	NA	NA	Please share Corrective measures taken by the client to prevent occurence in future.	NIL.
39	NA	NA	Please share Policy Copy for Policy Period from 31st March 2021 to 30th March 2022	Bidder to comply with GeM bid terms. The policy wordings mentioned in GeM bid is inline with exsiting policy.
40	NA	NA	Have you implemented a procedure to permanently comply with all privacy relevant legislative statutory, regulatory and contractual requirements?	Yes
41	NA	NA	Do you have guidelines issued on the retention, storage, handling and disposal of records and information?	Yes
42	NA	NA	Have you assigned a responsible person for providing guidance and ensuring awareness of privacy principles (e.g. Data Privacy Officer DPO)?	No
43	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. Internal every Six month & external annually
44	NA	NA	What is the coverage of VAPT? When was the same last done?	All Critical Assets. 2021-22
45	NA	NA	Have you conducted a Business Impact Analysis (BIA) ?	Yes
46	NA	NA	Do you have a Business Continuity Management (BCM) plan in place that specifically addresses cyber incidents?	Yes
47	NA	NA	Do you test your information security continuity plans (e.g. Business Continuity Management, Disaster Recovery) at least annually?	Yes
48	NA	NA	Are your information processing facilities (i.e. any system, service or infrastructure, or physical location housing it) implemented with redundancy?	Yes
49	NA	NA	What is the maximum acceptable outage or also known as RTO (Recovery Time Objective) for cyber systems? Please provide details on the same.	RTO is 2 hours for critical applications
50	NA	NA	Do you have an information security incident response plan in place?	Yes
51	NA	NA	Do all your employees and third party providers know the reporting line for information security events?	Yes
52	NA	NA	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	Have you established an escalation procedure for information security incidents?	Yes

D.I.T. Wi [illegible] Gr [illegible]
CAN BANK

Replies to Prebid Queries for GEM/2022/B/1853849 dated 12/01/2022 for selection of insurer for renewal of cyber risk insurance policy for Canara Bank from 31st march 2022 to 30th march 2023

Sl.No.	GeM bid clause	Clause/ Requirement	Bidder Query	Bank's Reply
54	NA	NA	Do you use knowledge gained from analysing and resolving information security incidents to reduce the likelihood or impact of future incidents?	Yes
55	NA	NA	Are any data centers / networks being shared between the entities / subsidiaries to be covered / even not covered under the policy please explain in detail?	No
56	NA	NA	Have you identified and documented all your important suppliers (including third party service providers)?	Yes
57	NA	NA	Do agreements with third party service providers require levels of security commensurate with your own information security standard?	Yes
58	NA	NA	Do you monitor third party service provider activities for cyber security events to maintain an agreed level of information security?	Yes
59	NA	NA	Does your web-server encrypt confidential data (e.g. HTTPS)?	Yes
60	NA	NA	Do you test security functionality during the development lifecycle of information systems incl. IT security updates?	Yes
61	NA	NA	Do you consider confidentiality when using operational data for testing to ensure that all sensitive details are protected by removal or modification?	Yes
62	NA	NA	Are all internet access points secured by appropriately configured firewalls?	Bank don't use Internet Access Points.
63	NA	NA	Do you monitor your network and identify security events?	Yes
64	NA	NA	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
65	NA	NA	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
66	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? Please explain intervlan security in detail?	Multiple Firewall are in place to filter inbound & outbound traffic (including business partner network)
67	NA	NA	Have you implemented change management procedures for critical systems?	Yes
68	NA	NA	Is the IT-environment for development and testing separated from production IT-environment?	Yes
69	NA	NA	Do you use malware protection for all web-proxies, email-gateways, workstations and laptops?	Yes
70	NA	NA	Besides traditional signature-based detection, does your malware protection use advanced heuristic- and behavioural-based detection mechanisms to protect against new malwares?	Yes
71	NA	NA	Do you perform at least weekly regular backups of business critical data?	Yes
72	NA	NA	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
73	NA	NA	Have you implemented a centralized software installation process?	Yes
74	NA	NA	Do you timely - at least within one month of release - apply updates to critical IT-systems and applications ("security patching")?	Yes
75	NA	NA	Do you technically or organisationally ensure that users must not install and, or run portable softwares on their workstations by themselves? (Excluding admin right restrictions)	Yes
76	NA	NA	Do you maintain a list of personnel (employees, vendors and visitors) with authorized access to your premises and sensitive security areas?	Yes
77	NA	NA	Is all confidential information stored on mobile devices (e.g. smart phones, and laptops) encrypted?	No
78	NA	NA	Have you developed and implemented a policy on the use, protection and lifetime of cryptographic keys?	Yes

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

Replies to Prebid Queries for GEM/2022/B/1853849 dated 12/01/2022 for selection of insurer for renewal of cyber risk insurance policy for Canara Bank from 31st march 2022 to 30th march 2023

Sl.No.	GeM bid clause	Clause/ Requirement	Bidder Query	Bank's Reply
79	NA	NA	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
80	NA	NA	Do you have a formal access provisioning process in place for assigning and revoking access rights?	Yes
81	NA	NA	Do you prohibit local admin rights on workstations for users?	Yes
82	NA	NA	Do you review user access rights at least annually?	Yes
83	NA	NA	Do you revoke all system access, accounts and associated rights after termination of users (incl. employees, temporary employees, contractors or vendors)?	Yes
84	NA	NA	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
85	NA	NA	Do you have PIM, PAM solution in place? If yes, please specify details including coverage of the same.	Yes, Enterpise Wide Coverage
86	NA	NA	Is multi factor authentication being used for all the cyber systems? If no what is the coverage of the same.	Yes
87	NA	NA	Are any of the manufacturing / logistic systems connected / dependant on IT systems which if not be working might result in any loss?	No
88	NA	NA	Do you keep an up-to-date inventory of software (incl. operating systems) and hardware assets in your network?	Yes
89	NA	NA	Do you classify information with regards to confidentiality?	Policy in place
90	NA	NA	Are information labelling procedures implemented in accordance with the above classification scheme?	No
91	NA	NA	Do you provide guidance on how to handle classified information?	Yes
92	NA	NA	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
93	NA	NA	Do you securely dispose media containing sensitive information if it is not used any longer?	Yes
94	NA	NA	Do you have a comprehensive Configuration Management Database (CMDB) including: all IT assets, public cloud assets, dependencies, criticality, ownership, software and patch versions? If yes, is it in house or vendor solution - please provide details on the same.	No. However, SCDs are in place
95	NA	NA	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
96	NA	NA	Do you have any User Behavioural Analytics tool (i.e., UEBA, etc.) to monitor patterns of human behaviour to detect anomalies from those patterns?	No
97	NA	NA	Have you assigned a responsible person for information security (e.g. Chief Information Security Officer "CISO")?	Yes
98	NA	NA	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
99	NA	NA	Please list all the security functions that exists (within the organization and via external vendor/MSP) to manage/perform day-to-day security tasks (example: SOC, TI, IR, etc.)	SOC & NOC is in place

D.I.T. Wing Procurement Group
CANARA BANK
Bengaluru - 56

Replies to Prebid Queries for GEM/2022/B/1853849 dated 12/01/2022 for selection of insurer for renewal of cyber risk insurance policy for Canara Bank from 31st march 2022 to 30th march 2023

Sl.No.	GeM bid clause	Clause/ Requirement	Bidder Query	Bank's Reply
100	NA	NA	Are any SaaS services being used /or provided? If yes who is responsible for the protection of data stored on the SaaS service being used? Please name the service provider.	Microsoft 365 for email
101	NA	NA	Please help with the future plans / improvements / roadmap for cyber security architecture including time frames to implement if any?	Details will be shared with the selected bidder
102	NA	NA	Have you developed and implemented a board approved information security policy which is corporate-wide and permanently available for all employees and relevant external parties?	Yes
103	NA	NA	Has the organization documented and implemented a cloud security policy to ensure security requirements are catered to when utilizing cloud services for business?	Yes
104	NA	NA	Does the organization timely, i.e. at least monthly, update IT systems and applications to prevent any known vulnerabilities being exploited? Or does the organization have a patch management solution to ensure that all critical and high-risk vulnerabilities reported are patched or mitigated within stipulated timeline?	Yes
105	NA	NA	Does the organization ensure that the default passwords on all computer systems (e.g. routers, etc) are changed to prevent entry in the organizations network through a brute force attack?	Yes
106	NA	NA	Does the organisation ensure high availability of business critical infrastructure to ensure business continuity in case of an incident?	Yes
107	NA	NA	Please elaborate in details. Does the organization have a Disaster Recovery (DR) site to allow it to continue business-sensitive operations in the event of a disaster? How many data centers does the organisation have? When was the last DR drill conducted.	Bank is having three Sites i.e. DC, DRC & NDR. Bank is conducting DR Drill to allow it to continue business sensitive operations as per board approved frequency. More details will be shared with the selected bidder
108	NA	NA	Does the organization have a dedicated Security Operations Center (SOC) that is capable of monitoring, reporting, investigating and recovering from any cyber security incident observed within the organization's network?	Yes
109	NA	NA	Does the organization have a Network Access Control (NAC) solution in place to allow the organization to restrict access to resources on their network and to prevent risk to the organization from Bring Your Own Device (BYOD), or the internet of things (IoT), or weak access permissions, or advanced persistent threats (APT), etc?	Yes
110	NA	NA	Has the organization implemented Deception Tool, or Honeypot solution to divert and detect attackers with no risk to real data, operations, or users?	Yes
111	NA	NA	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
112	NA	NA	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 behaviour?	Yes
113	NA	NA	Has the organization implemented an applications / softwares whitelisting solution on end-user devices and servers to limit the use of only authorized applications / softwares on the assets(excluding admin right restriction)?	Yes
114	NA	NA	Has the organization implemented a Intrusion Detection and Prevention (IDS/IPS) solution for network, and host to detect or prevent any malicious activity on IT assets by monitoring the network traffic?	Yes
115	NA	NA	Has the organization implemented a Data Loss Prevention (DLP) tool 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 monitoring mode

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

Replies to Prebid Queries for GEM/2022/B/1853849 dated 12/01/2022 for selection of insurer for renewal of cyber risk insurance policy for Canara Bank from 31st march 2022 to 30th march 2023

Sl.No.	GeM bid clause	Clause/ Requirement	Bidder Query	Bank's Reply
116	NA	NA	Does the organization have a Next-Generation Firewall (NGFW) or Unified Threat Management (UTM) solution capable of in-line Deep Packet Inspection (DPI) and an Intrusion Prevention System (IPS) in place to reduce risks arising from network vulnerabilities?	Yes
117	NA	NA	Does the organization ensure only secured connections like VPN are utilized for remote users to ensure the confidentiality of sensitive information in transit?	Yes
118	NA	NA	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
119	NA	NA	Has the organization implemented a Database Activity Monitoring (DAM) Solution to detect and prevent malicious behaviour in the database?	Yes
120	NA	NA	Has the organization implemented anti-Distributed Denial-of-Service (DDoS) solution to prevent DDoS attacks?	Yes
121	NA	NA	What is the frequency of backup? How are backups taken? What is the backup coverage including strategy? Please elaborate in details.	Data Backup Process is in place as per Bank's policy. Details will be shared with the selected bidder
122	NA	NA	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
123	NA	NA	When were the WAF rules last updated? Were rules added to WAF solution, to prevent log4j vulnerabilities from being exploited? Please respond in details	Yes
124	NA	NA	Are any apache, or applications based on java being used in the organisation? When were they last updated to the latest version available?	Yes
125	NA	NA	Training 1. Does the applicant conduct mandatory information security training at least annually for employees and contractors? 2. Does the applicant conduct mandatory privacy training at least annually for employees and contractors? 3. Select all contents that apply a. Security / threat awareness b. Social Engineering / Phishing c. Privacy / data handling compliance d. Role based training e. Attack Simulation	Yes
126	NA	NA	Patch management 1. Is patch management process in place for when patches must be deployed? 2. How quickly the critical patches applied a. Within 24 hours. b. 24-72 hours. c. 3-7 days. d. >7 days. 3. Are KPIs defined to track year to date patches deployment? a. >95% b. 90-95% c. <90% d. <80% e. No KPIs 4. Are legacy and end of life software segregated from the rest of the network? 5. Are security patches prioritised and tested prior to deployment?	Yes. Details will be shared with the selected bidder

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

Sl.No.	GeM bid clause	Clause/ Requirement	Bidder Query	Bank's Reply
127	NA	NA	Backups 1. Is documented backup policy in placed and enforced? 2. Are backups restored and tested for critical systems and data (including all systems, applications, databases, etc. that affect may lead to a business interruption) at least annually? 3. What is restore and test frequency? a. Monthly b. Quarterly c. Annually. 4. Are backups stored offline? If so, stored on site or offsite? And what is offsite storage frequency? Monthly, quarterly, annually. 5. Where are backups stored a. Cloud (online), b. On site, c. Offsite storage d. Other 6. Are backups encrypted and segmented?	Yes. Details will be shared with the selected bidder
128	NA	NA	IRP, BCP, DRP 1. Is documented disaster recovery plan in place and tested at least annually? 2. Is documented business continuity plan in place and tested at least annually? 3. Is documented incident response plan in place and tested at least annually? 4. How long before a critical system, application or data becomes unavailable will have materially impact on revenue? a. Immediately b. 1 - 4 hours. c. Up to 8 d. More than 24 hours 5. What is the Recovery Time Objective (RTO) for critical systems? a. Less than 1 hr b. 1 - 4 hours c. Up to 8 d. None defined 6. Do BCP, DRP processes include support agreements with vendors?	Yes. Details will be shared with the selected bidder
129	NA	NA	Monitoring and detection 1. Does the organisation have a Security Operations Centre? Is it internal or 3rd party Managed Security Service Provider? 2. Does the organisation utilise a. security information and event monitoring (SIEM) b. Data loss prevention (DLP) c. Intrusion detection and/or prevention solution (IDS/IPS) d. WAF, NGFW 3. Does the organisation monitors network traffic for anomalous and potentially suspicious data transfers? 4. Are security tools user behavioural and anomalies detection and exploit mitigation capabilities utilised?	Yes

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

Replies to Prebid Queries for GEM/2022/B/1853849 dated 12/01/2022 for selection of insurer for renewal of cyber risk insurance policy for Canara Bank from 31st march 2022 to 30th march 2023

Sl.No.	GeM bid clause	Clause/ Requirement	Bidder Query	Bank's Reply
130	NA	NA	Access Control 1. Is access control policy in place? Does it include password strength and rotation? 2. Does the applicant actively monitor all administrator access for unusual behaviour patterns? 3. Throughout the organisation are following solutions implemented a. Identity and access management b. Privileged access management 4. Do administrators have a unique, privileged credentials for administrative tasks which are separate from their user credentials for everyday access, email, etc.	Yes
131	NA	NA	Multifactor authentication (MFA) 1. Are all-external accesses including remote work, maintenance, third-party vendors to the corporate network and resources is permitted only through multifactor authentication (MFA)? 2. Is VPN by default utilised in addition to the multi-factor authentication for all remote accesses to corporate resources? 3. Is Remote Desktop Protocol (RDP) enabled? If yes, is access restricted only through VPN, network level authentication and Multifactor authentication (MFA)? 4. Is Multi factor authentication (MFA) required for accessing a. Critical data or application b. domain administrators c. privileged user access	Yes
132	NA	NA	Network segregation 1. Are physical and/or logical network segregations ensured for all 1. business-critical systems 2. data centres 3. backup and production environments 4. Wi-Fi and guest networks 2. Is network segregated by geography to prevent lateral movement? 3. Are networks segmented by business functions? 4. By default, 1. do firewall rules prevent RDP use and disallow inbound connections 2. are all service accounts configured to deny interactive logons 5. Is microsegmentation or zero trust framework adopted to reduce overall attack surface	Yes
133	NA	NA	Encryption 1. Do all portable devices use full disk encryption? 2. Is critical and sensitive data encrypted while at rest? 3. Is critical and sensitive data encrypted while in motion? 4. Is critical and sensitive data encrypted while in transit?	Yes
134	NA	NA	Governance 1. Are cybersecurity governance processes in place with clearly defined responsibilities for IT-/Information security and covering third-party services providers? 2. Does the organisation follow information security standards or framework such as ISO 27001, NIST? If so, are they certified to these standards? 3. Are internal and/or external cyber security audits performed at least annually?	Yes

D.I.T. Wing, Procurement Gr.
CANARA
Bengaluru-560

Replies to Prebid Queries for GEM/2022/B/1853849 dated 12/01/2022 for selection of insurer for renewal of cyber risk insurance policy for Canara Bank from 31st march 2022 to 30th march 2023

Sl.No.	GeM bid clause	Clause/ Requirement	Bidder Query	Bank's Reply
135	NA	NA	Mergers and acquisitions 1. Is due diligence and risk management process in place to cover cybersecurity assessment for mergers and acquisitions? 2. Do M&A cyber security processes dictate a staged (tiered) network integration to make sure the new entity is at least a comparable level of security to the policy holder? Are the networks kept entirely separated until such elevated cybersecurity levels?	Yes
136	NA	NA	Anti-malware measures 1. Does the organisation employ one or more endpoint security tools? Select all that apply a. Extended detection and response (XDR solution platform) b. Endpoint Detection Response (EDR) c. Endpoint Protection Platforms (EPP) 2. Are integrity tests of back-ups prior to restoration performed to ensure they are free from malware? 3. What % of the enterprise is covered by scheduled vulnerability scans? 4. Are penetration tests performed at least annually for the externally facing systems. 5. Does the organisation use external sources (threat intelligence companies, government agencies) to monitor its attack surface (external or internet facing systems)?	Yes, except EDR & XDR
137	NA	NA	6. Are following email security solutions enforced? Select all that are applicable a. Sender Policy Framework (SPF) b. DKIM (DomainKeys Identified Mail) c. Domain-based Message Authentication, Reporting and Conformance (DMARC) 7. Are email gateways configured to look for potentially malicious links, programs, and block executables? 8. Is web-based content filtering enforced with restricting access to social media sites, platforms? 9. Are macros disabled by default? 10. Are ransomware specific incident response processes in place? 11.Are ransomware scenarios tested at least annually?	Yes
138	NA	NA	COVID Questions: 1• Are the remote connections restricted to company supplied secure equipment? Is there adequate capacity to facilitate a sudden increase in volume of remote workers and maintain remote access to all critical infrastructure? 2• Please confirm that all necessary IT security measures including VPN, MFA etc. are implemented for the remote connections. 3• Are remote access control (request, obtain, use, terminate) policies and procedures being updated enabling staff to regularly work remotely on a formal basis? 4• Are communication channels and collaboration frequency enhanced to prevent remote employees vulnerable to disinformation (to take advantage of fears over coronavirus) related to COVID 19 cyber threets?	Yes

Procurement Group
C/IAP
Bengaluru-560001

Sl.No.	GeM bid clause	Clause/ Requirement	Bidder Query	Bank's Reply
139	NA	NA	Additional clarifications : - 1.As per the Apache advisory for CVE-2021-44228 vulnerability, are all upgrade, workarounds (setups, properties, environment variables, flags changes, blocks) and remediation measures implemented in order to prevent lookups in log event messages including earlier versions? 2.Are extensive searches carried out inside EAR, JAR and WAR files to determine Log4j installations including the dependent libraries within Java applications? If yes, please confirm the vulnerabilities are rectify through updates or circumventions. 3.Has the insured completed an impact/risk assessment for the Log4j 2 exploitation? 4.Are internet-facing applications prioritise for patching and isolated where necessary? Are internal critical instances of Log4j given precedence for patching over non-critical?	Details will be shared with the selected bidder
140	NA	NA	5.Please confirm the legacy Log4j systems software and applications are identified and "ringfence" until replacement, to reduce the security risk. 6.Are firewall, specially WAF if applicable, rules updated for Log4j 2 vulnerability (Remote Command Execution and inspect requests' headers, URI, and body etc.)? 7.Are advises from the security vendors, government advisories, protection bulletins strictly followed? 8.To reduce the attack surface are range of measures initiated? E.g., restricted outbound connections and programs execution, user access restrictions and rights limitation, network segregation mentation 9.If the servers are connected to the internet, are LDAP and RMI outbound traffic blocked, where possible? Are internally initiated LDAP connections to external destinations observed recently?	Details will be shared with the selected bidder
141	NA	NA	10.Has the insured in active discussion with its suppliers, software vendors to see if they have identified and remediated the Log4j vulnerability in their environment? If not, as a precautionary measures are Apache advisory for CVE-2021-44228 vulnerability followed thoroughly? 11.Are possible Log4j exploitation behaviours (suspicious remote PowerShell execution, obfuscated command/script launched, network traffic connection to C2 server) triaged and remediated immediately? 12.Has the insured initiated any forensic analysis to identify any IOC (Indicator of Compromise) resulting from the CVE-2021-44228 security flaw? If any IOC's were identified has the insured remediated and removed any identified malware in the insured computer system? What remedial actions are taken so far?	Details will be shared with the selected bidder
142	NA	NA	13.Is the insured aware of or advised by any of its critical vendors that they use the affected products,-applications or service identified in CVE-2021-44228 vulnerability? 14.Is any of the software (products, applications, and plug-ins) developed by the organisation vulnerable to the CVE-2021-44228? If so, has it been communicated with all affected customers to enable them to apply mitigations or install updates where they are available?	Details will be shared with the selected bidder

D.I.T. Wi. Procurement Group ★ Bengaluru-560 001 ★ CANARA

Replies to Prebid Queries for GEM/2022/B/1853849 dated 12/01/2022 for selection of insurer for renewal of cyber risk insurance policy for Canara Bank from 31st march 2022 to 30th march 2023

Sl.No.	GeM bid clause	Clause/ Requirement	Bidder Query	Bank's Reply
143	NA	NA	With respect to the Applicant's efforts to mitigate phishing, select all that apply 1.Applicant provides security awareness training to employees at least annually. 2.Applicant uses simulated phishing attacks to test employees' cybersecurity awareness at least annually. 3.Where the Applicant is conducting simulated phishing attacks, the success ratio was less than 15% on the last test (less than 15% of employees were successfully phished). 4.Applicant 'tags' or otherwise marks e-mails from outside the organization. 5.Applicant has a process to report suspicious e-mails to an internal security team to investigate. None of the above. Additional Commentary on efforts to mitigate phishing:	Yes
144	NA	NA	Does the Applicant have a documented process to respond to phishing campaigns (whether targeted specifically at the Applicant or not)? Yes No If "Yes", please describe the principal steps to respond:	Yes. Details will be shared with the selected bidder
145	NA	NA	With respect to the Applicant's efforts to block potentially harmful websites and/or email, select all that apply: 1.Applicant uses an e-mail filtering solution which blocks known malicious attachments and suspicious file types, including executables. 2.Applicant uses an e-mail filtering solution which blocks suspicious messages based on their content or attributes of the sender. 3.Applicant uses a web-filtering solution which stops employees from visiting known malicious or suspicious web pages. 4.Applicant uses block uncategorized and newly registered domains using web proxies or DNS filters. 5.Applicant uses a web-filtering solution which blocks known malicious or suspicious downloads, including executables. 6.Applicant's e-mail filtering solution has the capability to run suspicious attachments in a sandbox. 7.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-based web filters or require a VPN connection to browse the internet). None of the above. Additional commentary on efforts to block malicious websites and/or email:	Yes

D.I.T. Wing, Procurement Gro
CANARA BANK
Bengaluru - 560 001

Replies to Prebid Queries for GEM/2022/B/1853849 dated 12/01/2022 for selection of insurer for renewal of cyber risk insurance policy for Canara Bank from 31st march 2022 to 30th march 2023

Sl.No.	GeM bid clause	Clause/ Requirement	Bidder Query	Bank's Reply
146	NA	NA	With respect to authentication for employees who are remotely accessing the corporate network and any cloud-based services where sensitive data may reside (including VPN access, and cloud-based email and CRM; together 'remote access to corporate resources'), select the description which best reflects the Applicant's posture: (As used herein, "multi-factor authentication" means authentication which uses at least two different types of the possible authentication factors (something you know, something you have, and something you are); the Applicant can provide further explanation below)" 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. Applicant does not provide remote access to employees. Additional commentary on authentication for employees:	Multi factor Authetication System in place
147	NA	NA	With respect to authentication for independent contractors and vendors who are remotely accessing the corporate network and any cloud-based services where sensitive data may reside (including VPN access, and cloud-based email and CRM; together 'remote access to corporate resources'), select the description which best reflects the Applicant's posture: (The Applicant can provide further explanation below)" 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. Applicant does not provide remote access to independent contractors/vendors. Additional commentary on authentication for independent contractors/vendors:	Multi factor Authetication System in place
148	NA	NA	Does the Applicant's multifactor authentication implementation also meet the criteria that the compromise of any single device will only compromise a single authenticator? (For illustration: where authentication requires a password (knowledge) and a token (possession), this would not meet the criteria above if the token to prove possession is kept on a device the password is also entered into, exposing both if the device is compromised)" A1.Not Applicable (Applicant does not use multi-factor authentication) A2.No; Applicant's multi-factor implementation does not meet the above criteria. A3.Yes; the Applicant's multi-factor implementation meets the above criteria. Additional commentary on Multi-factor authentication implementation:	Multi factor Authetication System in place

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

Replies to Prebid Queries for GEM/2022/B/1853849 dated 12/01/2022 for selection of insurer for renewal of cyber risk insurance policy for Canara Bank from 31st march 2022 to 30th march 2023

Sl.No.	GeM bid clause	Clause/ Requirement	Bidder Query	Bank's Reply
149	NA	NA	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. Applicant uses endpoint security tools with behavioral-detection and exploit mitigation capabilities. Applicant has an internal group which monitors the output of endpoint security tools and investigates any anomalies. None of the above. Additional commentary on endpoint security capabilities:	Yes
150	NA	NA	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 below) 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. Additional commentary on security monitoring:	24*7 Monitoring done in SOC
151	NA	NA	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 <30 minutes 30 minutes-2 hours 2-8 hours >8 hours Additional commentary on average time to remediate:	Not applicable as there were no security incidents in the period. However, standalone security incidents observed at few ATMs.
152	NA	NA	With respect to access controls for each user's workstation, select the description which best reflects the Applicant's posture: (The Applicant can provide further explanation below)" 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. Some of Applicant's employees are in the Administrators' group or are local admins. Do not know. Additional commentary on access controls for workstations:	By default general users are not having admin previleges. Only designated personnel perform adminsitrator functions.

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

Replies to Prebid Queries for GEM/2022/B/1853849 dated 12/01/2022 for selection of insurer for renewal of cyber risk insurance policy for Canara Bank from 31st march 2022 to 30th march 2023

Sl.No.	GeM bid clause	Clause/ Requirement	Bidder Query	Bank's Reply
153	NA	NA	With respect to protecting privileged credentials, select all that apply with respect to the Applicant's posture: 1-System administrators at the Applicant have a unique, privileged credential for administrative tasks (separate from their user credentials for everyday access, email, etc.). 2-Privileged accounts (including Domain Administrators) require multifactor authentication. 3-Privileged accounts are kept in a password safe that require the user to "check out" the credential (which is rotated afterwards). 4-There is a log of all privileged account use for at least the last thirty days. 5- Privileged Access Workstations (workstations that do not have access to internet or e-mail) are used for the administration of critical systems (including authentication servers/ Domain Controllers)." None of the above. Additional commentary on protecting privileged credentials:	Privileged accounts (including Domain Administrators) require multifactor authentication.
154	NA	NA	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): "Number of service accounts in the Domain Administrators group: (""service account"" means a user account created specifically for an application or service to interact with other domain-joined computers):" Additional commentary on the number of Domain Administrators:	Bank uses Microsoft Active Directory. Details will be shared with the selected bidder
155	NA	NA	How many users have persistent privileged accounts for endpoints (servers and workstations)? (For the purposes of this question, "privileged accounts" means entitlements to configure, manage and otherwise support these endpoints; users who must 'check out' credentials should not be included. The Applicant can provide further explanation below)" Please enter an integer: Additional commentary on the number of privileged accounts:	Details will be shared with the selected bidder
156	NA	NA	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. Applicant has a Web Application Firewall (WAF) in front of all externally facing applications, and it is in blocking mode. Applicant uses an external service to monitor its attack surface (external/internet facing systems). None of the above.	Yes. All three in place

Replies to Prebid Queries for GEM/2022/B/1853849 dated 12/01/2022 for selection of insurer for renewal of cyber risk insurance policy for Canara Bank from 31st march 2022 to 30th march 2023

Sl.No.	GeM bid clause	Clause/ Requirement	Bidder Query	Bank's Reply
157	NA	NA	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. 24-72 hours. 3-7 days. > 7 days. Additional commentary on target times for patching: Critical patches/security patches are deployed as and when required	Details will be shared with the selected bidder
158	NA	NA	What is the Applicant's year to date compliance with its own standards for deploying critical patches? (The Applicant can provide further explanation below)" Applicant does not track this metric/Do not know >95% 90-95% 80-90% <80% Additional commentary on patching compliance:	Details will be shared with the selected bidder
159	NA	NA	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. Applicant monitors network traffic for anomalous and potentially suspicious data transfers. Applicant monitors for performance and storage capacity issues (such as high memory or processor usage, or no free disk space). Applicant has tools to monitor for data loss (DLP) and they are in blocking mode. None of the above. Additional commentary on network monitoring:	Yes, All are in place
160	NA	NA	With respecting to limiting lateral movement, select all that apply to the Applicant's posture: (The Applicant can provide further explanation below)" 1.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). 2.Applicant has segmented the network by business function (e.g. traffic between asset supporting different functions - HR and Finance for example - is denied unless required to support a specific business requirement). 3.Applicant has implemented host firewall rules that prevent the use of RDP to log into workstations. 4.Applicant has configured all service accounts to deny interactive logons. None of the above. Additional commentary on segmentation:	Yes All four in place
161	NA	NA	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.	As part of Table Top exercise the scenarios pertaining to ransomware exercise are also being discussed.

D.I. Wing Procurement Group ★ C NARA ★ Bengaluru - 560 01

Replies to Prebid Queries for GEM/2022/B/1853849 dated 12/01/2022 for selection of insurer for renewal of cyber risk insurance policy for Canara Bank from 31st march 2022 to 30th march 2023

Sl.No.	GeM bid clause	Clause/ Requirement	Bidder Query	Bank's Reply
162	NA	NA	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 Yes 3rd party ransomware response principle steps: No. But regular backup inplace for critical applications	No
163	NA	NA	"With regards to verifying the efficacy of security controls, select all that apply to the Applicant: (The Applicant can provide further explanation below)" 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. 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:	Bank has an internal "red team" that tests security controls and response. Bank has engaged an external party to simulate threat actors and test security controls in the last year.
164	NA	NA	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. 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.	Yes, Both are in place
165	NA	NA	What is the Applicant's Recovery Time Objective (RTO) for critical systems? Applicant does not have an RTO/Does not know < 4 hours. 4-24 hours. 1 to 2 days. 2-7 days.	< 4 hours
166	NA	NA	With respect to backup capabilities, select all that apply to the Applicant: 1.Applicant's backup strategy includes offline backups (can be stored on site) 2.Applicant's backup strategy includes offline backups stored offsite 3.Applicant's backups can only be accessed via an authentication mechanism outside of our corporate Active Directory. Additional commentary on backup capabilities:	Applicant's backup strategy includes offline backups stored offsite
167	NA	NA	Does the Applicant have a policy that all portable devices use full disk encryption? Yes No Additional commentary:	Yes
168	NA	NA	Information Security Policy	Yes
169	NA	NA	Business Continuity Plan/Disaster Recovery Plan	Yes

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

Replies to Prebid Queries for GEM/2022/B/1853849 dated 12/01/2022 for selection of insurer for renewal of cyber risk insurance policy for Canara Bank from 31st march 2022 to 30th march 2023

Sl.No.	GeM bid clause	Clause/ Requirement	Bidder Query	Bank's Reply
170	NA	NA	Last 3 years premium & claim statistics	Currently, the claim is under process with the insurer and insurer has created reserves for Rs.22.75 Lakhs and final survey report is awaited. Bidder to comply with GeM bid terms.
171	NA	NA	Brief description of the claim, if any	The claim is releated to standalone security incidents observed at few ATMs. The financial loss amounting to Rs.72.75 Lakhs.
172	NA	NA	Preventive measures taken after the claim, if any	Bank has implemented TLS 1.2 encryption in all ATMs for encrypted communication between ATM Switch and ATM machine.
173	NA	NA	Whether 24*7 SOC is present	Yes
174	NA	NA	Whether data monitoring is performed	Yes
175	NA	NA	Frequency of updating malwares/security patches	Yes, as and when OEM released and patching is being done on monthly basis
176	NA	NA	Frequency of back up data testing/recovery process	Half Yearly
177	NA	NA	Frequency of audit/ review of privilege user access rights	Monthly
178	NA	NA	Frequency of audit log generation and validation of those logs	As per Bank's policy
179	NA	NA	Are network devices configured securely	Yes
180	NA	NA	Whether secure remote access connectivity is provided	Yes
181	NA	NA	Whether client is using fully updated web browser and email in the organisation	Yes
182	NA	NA	Whether security assessment for in-house and third party procured web/phone application is performed	Yes
183	NA	NA	Is incident response plan present and tested in case of cyber emergency	Yes
184	NA	NA	Data breach incident - If any	However, there were no security incidents in the period. However, standalone security incidents observed at few ATMs.
185	NA	NA	2.Claims details and ICR for the last three years	Currently, the claim is under process with the insurer and insurer has created reserves for Rs.22.75 Lakhs and final survey report is awaited. Bidder to comply with GeM bid terms.
186	NA	NA	3. Any variation from Expiring insurance Coverage details.	The broad scope of cover remains as the expiring policy. Bidder to comply with GeM bid terms.
187	NA	NA	Steps taken by the company to prevent potential Data Breach incidents due to all/most employees working from home?	Details will be shared with the selected bidder
188	NA	NA	1.Is there a BCP plan in place? 2.Has the BCP been tested for a scenario where all/most employees must work either from home or alternate locations? 3.Has the Insured discussed their BCP with their regulators, and if yes what has been the response?	Yes
189	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 impact measured and assessed?	Normal
190	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, its maintained

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

Replies to Prebid Queries for GEM/2022/B/1853849 dated 12/01/2022 for selection of insurer for renewal of cyber risk insurance policy for Canara Bank from 31st march 2022 to 30th march 2023

Sl.No.	GeM bid clause	Clause/ Requirement	Bidder Query	Bank's Reply
191	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.	Yes
192	NA	NA	Has the regulator imposed any restrictions on the insured whilst operating under their alternative operating environment pursuant to their BCP?	No
193	NA	NA	Are employees allowed to use personal devices for official usage?	No
194	NA	NA	1.Is webmail accessible outside corporate network? If yes, How is access to emails protected? 2.Are the remote connections restricted to company supplied secure equipment? 3.Is there adequate capacity to facilitate a sudden increase in volume of remote workers and maintain remote access to all critical infrastructure? 4.Are remote access control (request, obtain, use, terminate) policies and procedures being updated enabling staff to regularly work remotely on a formal basis?	1. Email solution is integrated with internal AD server. 2.No 3.Yes 4.Yes
195	NA	NA	Do you have log monitoring?	Yes
196	NA	NA	How often and in what way is cyber security awareness training provided to your employees?	Security awareness workshops/phishing simulation exercises/quizzes etc., are conducted regularly by the bank for all stake holders
197	NA	NA	What redundancies do you leverage in the design of your infrastructure? (Eg automatic failover logic, IT systems in HA mode). What kind of redundancies do you leverage for your mission critical systems ? Are you on a hot or warm site standby?	All Critical Application is designed in High Availability. Further DR Site is Hot Site.
198	NA	NA	Please provide details on protection measures implemented to secure electronic data stored or accessed or processed on end user systems and servers from information security breaches?	Encryption at rest & trasit is in place
199	NA	NA	1.Is two factor authentication enabled for critical systems and cloud services? - 2.Which IT-relevant third party products / services does your company purchase? Supplier Quality Assurance, Qualification of HW, SW and Services? 3.Does your company use any external Cloud solution? If yes, please specify. If global presence - please list your internet providers incl. contractual bandwidth capacity.	Details will be shared with the selected bidder
200	NA	NA	Were there any critical findings in the VAPT testing? Have all the findings been implemented? How frequently is VAPT conducted?	Yes. Internal every Six month & external annually. More details will be provided to selected bidder
201	NA	NA	Has the organization performed a DR drill to ensure the effectiveness of its disaster recovery plan?	Yes
202	NA	NA	What is the maximum acceptable outage or also known as RTO (Recovery Time Objective) for critical systems? Are any cloud service providers being used? If yes which? are these time objectives tested at least annually?	2 Hours
203	NA	NA	1.Is application white listing implemented on end-user devices and servers to limit the use of only authorized applications? 2.Is data at rest and transit encrypted?	Yes
204	NA	NA	1.Are SDLC methods followed while software development / customization? 2.Are any saas services being used /or provided? IF yes who is responsible for the protection of data stored on the saas service?	Yes
205	NA	NA	Is the organisation GDPR compliant?	Not Applicable
206	NA	NA	Update on the IT integration of the acquired banks by Canara bank. Is the IT integration complete and are the acquired banks on the Canara Bank IT Security Systems.	Yes
207	NA	NA	Please provide BCP copy	Details will be shared with the selected bidder

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

Replies to Prebid Queries for GEM/2022/B/1853849 dated 12/01/2022 for selection of insurer for renewal of cyber risk insurance policy for Canara Bank from 31st march 2022 to 30th march 2023

Sl.No.	GeM bid clause	Clause/ Requirement	Bidder Query	Bank's Reply
208	NA	NA	In case BCP can't be shared please provide the following : - 1• List the process elements of your Business Continuity Planning (internal & external). BCP: Continuity of business activity and service delivery under crisis situation 2• Describe the risk management structure (including threat modelling and vulnerability controlling), established in your company 3• What would be the average daily Business Interruption (incl. Reconstitution costs) loss in case of a Cyber event (considering the critical locations)? 4• How comprehensive is your Cyber Incident Response Plan (CIRP)? How often is it tested?	Details will be shared with the selected bidder
209	NA	NA	How many severe (business critical) Cyber incidents are detected in a week and reported to the management?	No business critical incidents are detected
210	NA	NA	What's (roughly) the ratio commercial vs open-source software/applications in your company?	Details will be shared with the selected bidder
211	NA	NA	Does your company operate its own electronic data processing centre? If yes, please provide country/city of the largest centre. Topology, Network, Data Centre & Infrastructure? DC: Tier-classification?	Details will be shared with the selected bidder
212	NA	NA	Personally Identifiable Information (PII) and Commercial Client Records 1.• Number of PII records held 2• Number of credit card transactions processed 3• PCI DSS compliant & level	Details will be shared with the selected bidder
213	NA	NA	Are communication channels and collaboration frequency enhanced to prevent remote employees vulnerable to disinformation (to take advantage of fears over coronavirus) related to COVID 19 cyber threats?	Details will be shared with the selected bidder
214	NA	NA	Are any servers / desktops accessible via remote connectivity i.e remote desktop, team viewer, etc.? If yes. How is access to those servers protected?	Details will be shared with the selected bidder
215	NA	NA	Confirmation regarding Dependency on IT a- IT should be available 24/7, availability target rate 99.9% b- IT should not be interrupted for more than 4 hrs a time c- IT may support 24 hr of interruption or more	Details will be shared with the selected bidder
216	NA	NA	Security Level a- Security Standard in each location is very high b- Security Standard is very high in many locations, high in others c- Security Standard medium to high in different locations.	Details will be shared with the selected bidder
217	NA	NA	Operational recovery procedure: description of the existing back-up procedures and capabilities?	Details will be shared with the selected bidder
218	NA	NA	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	Details will be shared with the selected bidder
219	NA	NA	Do you test updates and upgrades of firmware, software, web-applications and products of your systems before deployment?	Yes
220	NA	NA	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
221	NA	NA	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
222	NA	NA	How is the network segregated (Please give detials on physical segreration , intervlan security, port blocking, inter-company, intra - company , etc)	Multiple Firewall are in place to filter inbound & outbound traffic (including business partner network)

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

Replies to Prebid Queries for GEM/2022/B/1853849 dated 12/01/2022 for selection of insurer for renewal of cyber risk insurance policy for Canara Bank from 31st march 2022 to 30th march 2023

Sl.No.	GeM bid clause	Clause/ Requirement	Bidder Query	Bank's Reply
223	NA	NA	are any of the manufacturing systems connected/dependant on IT systems which is not wokring might result in a manufacutring loss?	Not Applicable
224	NA	NA	Please help with the future plans/improvements for cyber security architecture including time frames to implement any ?	Details will be shared with the selected bidder
225	NA	NA	How are netoworks, servers, applications monitered for any cyber security incidents ?	Through SOC
226	NA	NA	Microsoft Questionnaire Has Insured/Applicant completed an impact/risk assessment of this event? Yes No Additional commentary:	Bidder query is not clear
227	NA	NA	In connection with the event, does the Insured/Applicant use any externally facing version of the product? Yes No Additional commentary:	Bidder query is not clear
228	NA	NA	Has Insured/Applicant patched the affected Microsoft Exchange Servers? Yes No if no, what is the expected date to complete the required updates? ____________________ Additional commentary:	Yes
229	NA	NA	If Insured/Applicant is unable to patch the affected Microsoft Exchange Servers, please indicate if any of the following Microsoft recommended mitigation techniques have been deployed (select all that apply) Implement an IIS Re-Write Rule to filter malicious https requests Disable Unified Messaging (UM) Disable Exchange Control Panel (ECP) Vdir Disable Offline Address Book (OAB) Vdir Additional commentary:	Not applicable
230	NA	NA	Has Insured/Applicant initiated any forensic analysis to identify any IOC (Indicator of Compromise) resulting from the identified security flaw? Yes No If yes, were any IOC's identified? Additional commentary:	No

D.I.T. Wing, Procurement * CANARA * Bengaluru-53

Replies to Prebid Queries for GEM/2022/B/1853849 dated 12/01/2022 for selection of insurer for renewal of cyber risk insurance policy for Canara Bank from 31st march 2022 to 30th march 2023

Sl.No.	GeM bid clause	Clause/ Requirement	Bidder Query	Bank's Reply
231	NA	NA	Has Insured/Applicant determined if any of its critical vendors use any affected Microsoft Exchange Server versions? Yes No If yes, please indication what actions have been taken (select all that apply) Critical vendors have been surveyed and Insured/Applicant is awaiting verification of impact Critical vendors have validated to Insured/Applicant that □ they do not use any of the affected versions and/or □ or have patched all affected versions of Microsoft Exchange. What percentage of vendors have completed responses ______% Critical vendors have advised Applicant/Insured that IoC have been identified in their environment related to this security flaw	Not applicable
232	NA	NA	1.Whether Breach Response Vendor is required to be mentioned in the policy ? 2.What is amended loss of personal information clause 3.What is amended forensic services ? 4.During WFH whether the laptops and gadgets are provided by the bank to all employees duly secured ? Attached questionnaires to be submitted duly filled in. Please let us know whether any changes in the covers / wordings, if any, as compared to exp.policy . Additional commentary:	1.Bank will provide a list of vendors to the successful insurer upon placement 2,3: " As per the policy wordings shared, pls refer endorsement......,. For further inputs/clarifications, kindly connect with GIB. 4.No
233	NA	NA	Implemented EDR solution (End Point Detection & Response) to all critical endpoints & servers	No
234	NA	NA	Implemented MFA (Multifactor Authentication) for: a) Remote Access into Corporate Network b) All Privileged/Administrator access c) Remote access into all Cloud based applications (Microsoft Office 365, Microsoft Azure, Workday, Salesforce etc.) d) Remote access into all corporate email systems (including Cloud based email systems, unless they are accessed via a VPN)	a) Yes b) Yes c) NA d) No
235	NA	NA	Limitation & Control of Network Ports a) RDP port has been disabled/closed b) SMB port has been disabled/closed	Details will be shared with the selected bidder
236	NA	NA	Implemented the following Email Security Controls a) Spam Filtering tools b) Email Authentication (SPF, DKIM, DMARC) c) Technology to alert email users of external vs internal emails d) Secure Email Gateway e) Sandboxing to analyze and block inbound email attachments with malicious behavior	Yes
237	NA	NA	Implemented Security Awareness Training & Phishing Exercises a) All Employees b) All Vendors	a) All Employees b) Vendors are covered as necessary.

I.T. Wing, Procurement Gr
CANARA BANK
Bengaluru-560 00

Replies to Prebid Queries for GEM/2022/B/1853849 dated 12/01/2022 for selection of insurer for renewal of cyber risk insurance policy for Canara Bank from 31st march 2022 to 30th march 2023

Sl.No.	GeM bid clause	Clause/ Requirement	Bidder Query	Bank's Reply
238	NA	NA	Implemented Microsoft Office 365 User best practices (if applicable) a) Enable the unified audit log and mailbox audit logging b) Configure and enable Data Loss Prevention (DLP) c) Enable Multifactor Authentication (MFA) d) Enable Office 365 Cloud Application Security e) Enable Microsoft Security Score	Yes
239	NA	NA	Ability to Disable Administrative Privilege on All Endpoints	Yes
240	NA	NA	Implemented Backup & Recovery Best Practices a) Regular incremental & full back up of key servers, applications and databases b) Backups are segmented/disconnected from corporate network c) Deploy multiple backup methods such as cloud storage & local backup d) Encrypt backups & segment encryption key	Yes
241	NA	NA	Maintain Regular Patch Management a) Follow Microsoft Patch Tuesday patches within 30 days b) Monthly vulnerability scans to ensure properly patched systems & applications c) Process to patch for the most commonly exploited CVE's published within 30 days	Yes
242	NA	NA	Formalize and Test Incident Response Plan Annually a) Established playbook for common incident affecting industry, such as BEC, Ransomware, Funds Transfer Fraud b) Establish process to use the FBI Financial Fraud Kill Chain to terminate and recover fraudulent electronic transfers	Yes
243	NA	NA	Has Insured/Applicant completed an impact/risk assessment of the following events noted below? 1.Apache Log4j vulnerability (CISA Emergency Directive 22-02) □YES □NO 2.Microsoft On Premise Exchange Server (CISA Emergency Directive 21-02 issued 3/3/21 □YES □NO 3.Ivanti Pulse Connect Secure Products (CISA Emergency Directive 21-03 issued 4/20/21 □YES □NO 4.Kaseya On Premise Server (CISA-FBI Guidance for MSPs and their Customers issued 7/4/21 □YES □NO 5.Microsoft Window Print Spooler (CISA Emergency Directive 21-04 issued 7/13/21 □YES □NO	Details will be shared with the selected bidder
244	NA	NA	Does the Insured/Applicant use any of the impacted software code, products or applications identified in any of these events? (check all that apply) □ Apache Log4j □ Microsoft On Premise Exchange Server □ Ivanti Pulse Connect Secure □ Kaseya On Premise VSA Server □ Enabled Microsoft Windows Print Spooler	Details will be shared with the selected bidder

D.I.T. Wing, Procurement Group ★ CANA ★ Bengaluru-560 001

Sl.No.	GeM bid clause	Clause/ Requirement	Bidder Query	Bank's Reply
245	NA	NA	Have all CVE's assigned to those vulnerabilities been remediated? 1.Apache Log4j (CISA Emergency Directive 22-02) □YES □NO □ N/A 2.Microsoft On Premise Exchange Server (CISA Emergency Directive 21-02 issued 3/3/21 □YES □NO □ N/A 3.Ivanti Pulse Connect Secure Products (CISA Emergency Directive 21-03 issued 4/20/21 □YES □NO □ N/A 4.Kaseya On Premise Server (CISA-FBI Guidance for MSPs and their Customers issued 7/4/21 □YES □NO □ N/A 5.Microsoft Window Print Spooler (CISA Emergency Directive 21-04 issued 7/13/21 □YES □NO □ N/A	Details will be shared with the selected bidder
246	NA	NA	Has Insured/Applicant initiated any forensic analysis to identify any IOC (Indicator of Compromise) resulting from the identified security flaw(s)? □YES □NO □N/A	Details will be shared with the selected bidder
247	NA	NA	Were any IOC's identified during the forensic analysis on any of the following products? (check only if identified) □ Apache Log4j □ Microsoft On Premise Exchange Server □ Ivanti Pulse Connect Secure □ Kaseya On Premise VSA Server □ Enabled Microsoft Windows Print Spooler	Details will be shared with the selected bidder
248	NA	NA	If any IOC's were identified has the Insured/Applicant remediated and removed any identified Malware in the Insured/Applicant's computer system for the following products? Apache Log4j vulnerability (CISA Emergency Directive 22-02) □YES □NO □ N/A Microsoft On Premise Exchange Server (CISA Emergency Directive 21-02 issued 3/3/21 □YES □NO □ N/A Ivanti Pulse Connect Secure Products (CISA Emergency Directive 21-03 issued 4/20/21 □YES □NO □ N/A Kaseya On Premise Server (CISA-FBI Guidance for MSPs and their Customers issued 7/4/21 □YES □NO □ N/A Microsoft Window Print Spooler (CISA Emergency Directive 21-04 issued 7/13/21 □YES □NO □ N/A	Details will be shared with the selected bidder
249	NA	NA	Does any of the Insured/Applicant's critical vendors use any of the affected products or applications identified in the events list above? □YES □NO □Unknown	Details will be shared with the selected bidder

D.I.T. Wing, Procurement G
CANARA
Bengaluru - 560 001

Replies to Prebid Queries for GEM/2022/B/1853849 dated 12/01/2022 for selection of insurer for renewal of cyber risk insurance policy for Canara Bank from 31st march 2022 to 30th march 2023

Sl.No.	GeM bid clause	Clause/ Requirement	Bidder Query	Bank's Reply
250	NA	NA	Has any of the Insured/Applicant's critical vendors advised the Applicant/Insured that IOC's have been identified in their environment related to these vulnerabilities? Apache Log4j vulnerability (CISA Emergency Directive 22-02) □YES □NO □ N/A Microsoft On Premise Exchange Server (CISA Emergency Directive 21-02 issued 3/3/21 □YES □NO □ N/A Ivanti Pulse Connect Secure Products (CISA Emergency Directive 21-03 issued 4/20/21 □YES □NO □ N/A Kaseya On Premise Server (CISA-FBI Guidance for MSPs and their Customers issued 7/4/21 □YES □NO □ N/A Microsoft Window Print Spooler (CISA Emergency Directive 21-04 issued 7/13/21 □YES □NO □ N/A	Details will be shared with the selected bidder
251	NA	NA	Has any of the Insured/Applicant's critical vendors advised the Applicant/Insured that their sensitive data has been compromised as a result of any of these events? Apache Log4j vulnerability (CISA Emergency Directive 22-02) □YES □NO □ N/A Microsoft On Premise Exchange Server (CISA Emergency Directive 21-02 issued 3/3/21 □YES □NO □ N/A Ivanti Pulse Connect Secure Products (CISA Emergency Directive 21-03 issued 4/20/21 □YES □NO □ N/A Kaseya On Premise Server (CISA-FBI Guidance for MSPs and their Customers issued 7/4/21 □YES □NO □ N/A Microsoft Window Print Spooler (CISA Emergency Directive 21-04 issued 7/13/21 □YES □NO □ N/A	Details will be shared with the selected bidder
252	NA	NA	Ransomware Strategy -Q12C Question 12C - "Number of service accounts in the Domain Administrators group: ("service account" means a user account created specifically for an application or service to interact with other domain-joined computers):"	Details will be shared with the selected bidder

Date: 29/01/2022
Place: Bangalore

Deputy General Manager

D.I.T. Procurement Group CANARA BANK H.O. B[illegible] 560 001