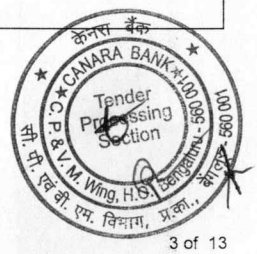
Replies to Pre bid Queries for GeM Bid ref. no: GEM/2025/B/5865415 dated 24/01/2025 for Selection of Insurer for Cyber Risk Insurance Policy for a Period of One Year from 31/03/2025 to 30/03/2026 in Canara Bank						
Sl. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Reply
1	NA	Generic	Generic	Generic	Please provide us with a list of major outsourcers for which cover is asked for? Are they cert-in certified outsourcers? Is there any pending PI issue/litigation/complaints from any of their vendors?	Major IT outsourcers provide services for implementation and maintenance of different solutions like BBPS, EJ, IaaS, PKI etc. , to name a few. There are no pending litigations.
2	NA	Generic	Generic	Generic	Please inform MFA implemented on all their external portals/web aggregators etc and when was the last VAPT carried out?	MFA is implemented for around 85% of our systems. As per bank policy, External VAPT is conducted half yearly through Cert In Empaneled Vendor. Last VAPT was on Jan 2025.
3	NA	Generic	Generic	Generic	Please inform whether software patch updation is automated ? If yes, please inform about the duration?	Yes. We have patch management system in place.Apart from OS patches and updates, patching for other third party software such as Edge, Chrome, Microsoft office,AV etc. are covered under automated patch update.
4	42	Annexure 2 - Pre Qualification Criteria	Sl. No: 2	**Qualification Criteria** The Bidder (including OEM and OSD/OSO, if any) should either be Class-I or Class-II local supplier as defined in Public Procurement (Preference to Make in India) Revised Order (English) dated 19/07/2024. **Documents to be submitted In compliance with Qualification Criteria** Certificate of local content to be submitted as per Annexure-4 as applicable.	Please waive off this point	Bidder to comply with RFP terms and conditions.

केनरा बैंक CANARA BANK Tender Processing Section C.P.&V.M. Wing, H.O. Bengaluru

Replies to Pre bid Queries for GeM Bid ref. no: GEM/2025/B/5865415 dated 24/01/2025 for Selection of Insurer for Cyber Risk Insurance Policy for a Period of One Year from 31/03/2025 to 30/03/2026 in Canara Bank						
Sl. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Reply
5	43	Annexure 2 - Pre Qualification Criteria	Sl. No: 4	**Qualification Criteria** If not a group of company, Bidder Company shall not be owned or controlled by any Director, or Key managerial personnel of the Canara Bank or their relatives. **Documents to be submitted In compliance with Qualification Criteria** Letter of Undertaking in company's letter head.	Please waive off this point	Bidder to comply with RFP terms and conditions.
6	43	Annexure 2 - Pre Qualification Criteria	Sl. No: 5	**Qualification Criteria** The bidder should provide confirmation that any person/ Partnership/ LLP/ Company including any subsidiary or holding company/ proprietorship connected to bidder directly or indirectly has not participated in the bid process. **Documents to be submitted In compliance with Qualification Criteria** The bidder should submit letter of confirmation on the Company's letter head to this effect.	Please waive off this point	Bidder to comply with RFP terms and conditions.

Replies to Pre bid Queries for GeM Bid ref. no: GEM/2025/B/5865415 dated 24/01/2025 for Selection of Insurer for Cyber Risk Insurance Policy for a Period of One Year from 31/03/2025 to 30/03/2026 in Canara Bank						
Sl. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Reply
7	43	Annexure 2 - Pre Qualification Criteria	Sl. No: 10	**Qualification Criteria** The bidder should have the minimum solvency ratio of 1.5% as on 31st March 2024 (This criteria is not applicable for PSU insurance companies) **Documents to be submitted In compliance with Qualification Criteria** Bidder must produce a certificate from the Company's Chartered Accountant/s /Company Secretary to this effect. The documents certified by Chartered Accountant/s should mandatorily contain Unique Document Identification Number.	Please waive off this point	Bidder to comply with RFP terms and conditions.
8	43	Annexure 2 - Pre Qualification Criteria	Sl. No: 11	**Qualification Criteria** The Net Worth of bidder should not be negative as on 31/03/2024 and also should have not been eroded more than 30% in the last three financial years ending on 31/03/2024. (This criteria is not applicable for PSU insurance companies) **Documents to be submitted In compliance with Qualification Criteria** The bidder should submit certificate from the Company's Chartered Accountant with UDIN to this effect.	Please waive off this point	Bidder to comply with RFP terms and conditions.



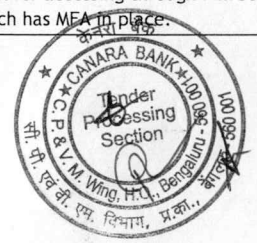
Replies to Pre bid Queries for GeM Bid ref. no: GEM/2025/B/5865415 dated 24/01/2025 for Selection of Insurer for Cyber Risk Insurance Policy for a Period of One Year from 31/03/2025 to 30/03/2026 in Canara Bank						
Sl. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Reply
9	44	Annexure 2 - Pre Qualification Criteria	Sl. No: 13	**Qualification Criteria** The Bidder should not be from a country which shares a land border with India unless the bidder is registered with the Competent Authority. **Documents to be submitted In compliance with Qualification Criteria** A declaration to be submitted in Company's letter head.	Please waive off this point	Bidder to comply with RFP terms and conditions.
10	NA	Generic	Generic	Generic	Whether there is any change in the terms of Insurance cover sought from the expiring Policy.	There has been sub-limit enhancement for some coverages. Kindly refer to the Scope of Work of the renewal RFP for the same.
11	NA	Generic	Generic	Generic	What is your approach to patching your environment? Can you please elaborate on how you are monitoring systems and what vulnerability assessment tools are available to you? and how do you keep the corporate environment up to date?	Patching is done as per the established SOPs, Policies and guidelines of the bank. Monitoring for malicious activities on the systems is carried out using 24x7 SOC solutions tools including PIM, SIEM and also through DAM, AV, etc. Bank also has a dedicated command centre team availble 24*7 for monitoring the performance of Network, servers, DBs public facing applications, ATM devices and related systems. We have inhouse vulnerability tools available for conducting VA periodically as per the policy. We maintain our environment upto date through regular patching, various security assessments, BCP procedures and drills, training and development, established policies and procedures, compliance and standards, enterprise applications and tools, vendor management, security controls etc.

Replies to Pre bid Queries for GeM Bid ref. no: GEM/2025/B/5865415 dated 24/01/2025 for Selection of Insurer for Cyber Risk Insurance Policy for a Period of One Year from 31/03/2025 to 30/03/2026 in Canara Bank						
Sl. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Reply
12	NA	Generic	Generic	Generic	What logging capabilities are available to you? and how long do you retain logs for?	System logs, DB logs and application logs are generated. Logs are further integrated and forwarded to SIEM also.Retention of Logs are as per our approved policy.
13	NA	Generic	Generic	Training	Does the applicant conduct mandatory information security training at least annually for employees and contractors?	Yes
14	NA	Generic	Generic	Training	Does the applicant conduct mandatory privacy training at least annually for employees and contractors?	Yes, Mandatory e learning module is provided and Circulating Educative series is published on fortnight basis to create Data privacy awareness among the employees.
15	NA	Generic	Generic	Training	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	a. Security / threat awareness- b. Social Engineering / Phishing c. Privacy / data handling compliance d. Role based training e. Attack Simulation
16	NA	Generic	Generic	Patch management	Is patch management process in place for when patches must be deployed?	Yes. SOP and policy in place
17	NA	Generic	Generic	Patch management	How quickly the critical patches applied a. Within 24 hours.- b. 24-72 hours. c. 3-7 days d. >7 days.	a. Within 24 hours
18	NA	Generic	Generic	Patch management	Are KPIs defined to track year to date patches deployment? a. >95%- b. 90-95% c. <90% d. <80% e. No KPIs	a.>95%
19	NA	Generic	Generic	Patch management	Are legacy and end of life software segregated from the rest of the network? They ensure that any end-of-life (legacy) vendor supplied software assets (including software, firmware etc.) in use is s adequately secured protected by mitigating controls.	Legacy systems are not used. End of Life software are used as long as it is under support.
20	NA	Generic	Generic	Patch management	Are security patches prioritised and tested prior to deployment?-	Yes
21	NA	Generic	Generic	Backups	Is documented backup policy in placed and enforced	yes

Replies to Pre bid Queries for GeM Bid ref. no: GEM/2025/B/5865415 dated 24/01/2025 for Selection of Insurer for Cyber Risk Insurance Policy for a Period of One Year from 31/03/2025 to 30/03/2026 in Canara Bank

Sl. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Reply
22	NA	Generic	Generic	Backups	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?	Yes
23	NA	Generic	Generic	Backups	What is restore and test frequency?- a. Monthly b. Quarterly c. Annually.	Half-yearly
24	NA	Generic	Generic	Backups	Are backups stored offline? If so, stored on site or offsite? And what is offsite storage frequency? Monthly, quarterly, annually.-	Yes. Backups are stored offline also. Backups are taken to both onsite and offsite locations. Backup storage frequency is according to the approved Backup guidelines of the bank.
25	NA	Generic	Generic	Backups	Where are backups stored a. Cloud (online), b. On site- c. Offsite storage - d. Other	b. On site c. Offsite storage
26	NA	Generic	Generic	Backups	Are backups encrypted and segmented?	Yes
27	NA	Generic	Generic	IRP, BCP, DRP	Is documented disaster recovery plan in place and tested at least annually?	Yes
28	NA	Generic	Generic	IRP, BCP, DRP	Is documented business continuity plan in place and tested at least annually?	Yes
29	NA	Generic	Generic	IRP, BCP, DRP	Is documented incident response plan in place and tested at least annually?	Yes
30	NA	Generic	Generic	IRP, BCP, DRP	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	The timeframe can vary depending on the specific applications
31	NA	Generic	Generic	IRP, BCP, DRP	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	b. 1 - 4 hours However, RTO can vary depending on the specific applications
32	NA	Generic	Generic	IRP, BCP, DRP	Do BCP, DRP processes include support agreements with vendors?	Yes

Replies to Pre bid Queries for GeM Bid ref. no: GEM/2025/B/5865415 dated 24/01/2025 for Selection of Insurer for Cyber Risk Insurance Policy for a Period of One Year from 31/03/2025 to 30/03/2026 in Canara Bank						
Sl. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Reply
33	NA	Generic	Generic	Monitoring and detection	Does the organisation have a Security Operations Centre? Is it internal or 3rd party Managed Security Service Provider?-	Yes. Internal
34	NA	Generic	Generic	Monitoring and detection	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-	The details utilised are a. security information and event monitoring (SIEM) - b. Data loss prevention (DLP) c. Intrusion detection and/or prevention solution (IDS/IPS)- d. WAF, NGFW
35	NA	Generic	Generic	Monitoring and detection	Does the organisation monitors network traffic for anomalous and potentially suspicious data transfers?-	Yes
36	NA	Generic	Generic	Monitoring and detection	Are security tools user behavioural and anomalies detection and exploit mitigation capabilities utilised?-	Yes
37	NA	Generic	Generic	Access Control	Is access control policy in place? Does it include password strength and rotation?	Yes
38	NA	Generic	Generic	Access Control	Does the applicant actively monitor all administrator access for unusual behaviour patterns?	Yes
39	NA	Generic	Generic	Access Control	Throughout the organisation are following solutions implemented- a. Identity and access management b. Privileged access management	Yes
40	NA	Generic	Generic	Access Control	Do administrators have a unique, privileged credentials for administrative tasks which are separate from their user credentials for everyday access, email, etc.-	Yes
41	NA	Generic	Generic	Multifactor authentication (MFA)-	Are all-external accesses including remote work, maintenance, third-party vendors to the corporate network and resources is permitted only through multifactor authentication (MFA)?	Yes
42	NA	Generic	Generic	Multifactor authentication (MFA)-	Is VPN by default utilised in addition to the multi-factor authentication for all remote accesses to corporate resources?	No
43	NA	Generic	Generic	Multifactor authentication (MFA)-	Is Remote Desktop Protocol (RDP) enabled? If yes, is access restricted only through VPN, network level authentication and Multifactor authentication (MFA)?	RDP access is disabled by default. However RDP Port is enabled at server level for accessing through PIM Solution, which has MFA in place.



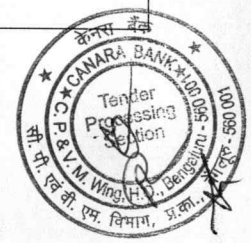
Replies to Pre bid Queries for GeM Bid ref. no: GEM/2025/B/5865415 dated 24/01/2025 for Selection of Insurer for Cyber Risk Insurance Policy for a Period of One Year from 31/03/2025 to 30/03/2026 in Canara Bank						
Sl. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Reply
44	NA	Generic	Generic	Multifactor authentication (MFA)-	Is Multi factor authentication (MFA) required for accessing a. Critical data or application- b. domain administrators- c. privileged user access-	Yes
45	NA	Generic	Generic	Network segregation	Are physical and/or logical network segregations ensured for all - business-critical systems data centres backup and production environments Wi-Fi and guest networks	Business-critical systems - YES Data centres - YES Backup and production environments - YES Wi-Fi and guest networks - NOT APPLICABLE
46	NA	Generic	Generic	Network segregation	Is network segregated by geography to prevent lateral movement?	Yes
47	NA	Generic	Generic	Network segregation	Are networks segmented by business functions?-	Yes
48	NA	Generic	Generic	Network segregation	By default, do firewall rules prevent RDP use and disallow inbound connections- are all service accounts configured to deny interactive logons	By default, firewall rules prevent RDP use and disallow inbound connections. Also, all service accounts configured to deny interactive logons
49	NA	Generic	Generic	Network segregation	Is microsegmentation or zero trust framework adopted to reduce overall attack surface?	We have multiple controls in place to reduce attack surface: Network Security: Firewalls, IPS, IDS, Anti-DDOS, NBA, ATP, NAC etc.System Security: AV,EDR, Patch Management, DLP etc. Application Security:SSO,WAF,MFA,RBAC etc.Identity Access & Management: PIM, AD, Biometric, TACACS, etc.Robust security policies.
50	NA	Generic	Generic	Encryption	Do all portable devices use full disk encryption? -	Devices that are enrolled with MDM will have a seperate work profile along with employee personal profile.No data can be shared outside work pfoile by the staff from these devices
51	NA	Generic	Generic	Encryption	Is critical and sensitive data encrypted while at rest?	Yes
52	NA	Generic	Generic	Encryption	Is critical and sensitive data encrypted while in motion?	Yes
53	NA	Generic	Generic	Encryption	Is critical and sensitive data encrypted while in transit?	Yes

Replies to Pre bid Queries for GeM Bid ref. no: GEM/2025/B/5865415 dated 24/01/2025 for Selection of Insurer for Cyber Risk Insurance Policy for a Period of One Year from 31/03/2025 to 30/03/2026 in Canara Bank						
Sl. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Reply
54	NA	Generic	Generic	Governance	Are cybersecurity governance processes in place with clearly defined responsibilities for IT-/Information security and covering third-party services providers? Does the organisation follow information security standards or framework such as ISO 27001, NIST? If so, are they certified to these standards?	Yes.Governance processes are in place with clear defined roles. Bank is certified with ISO 27001:2022
55	NA	Generic	Generic	Governance	Are internal and/or external cyber security audits performed at least annually?-	Yes
56	NA	Generic	Generic	Mergers and acquisitions	Is due diligence and risk management process in place to cover cybersecurity assessment for mergers and acquisitions?-	Yes
57	NA	Generic	Generic	Mergers and acquisitions	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
58	NA	Generic	Generic	Anti-malware measures	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)	EDR and EPP
59	NA	Generic	Generic	Anti-malware measures	Are integrity tests of back-ups prior to restoration performed to ensure they are free from malware?	Yes
60	NA	Generic	Generic	Anti-malware measures	What % of the enterprise is covered by scheduled vulnerability scans?	All the IT assets of the bank is covered by vulnerability scans
61	NA	Generic	Generic	Anti-malware measures	Are penetration tests performed at least annually for the externally facing systems.	Yes
62	NA	Generic	Generic	Anti-malware measures	Does the organisation use external sources (threat intelligence companies, government agencies) to monitor its attack surface (external or internet facing systems)?	Yes
63	NA	Generic	Generic	Anti-malware measures	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)	a. Sender Policy Framework (SPF) b. DKIM (DomainKeys Identified Mail) c. Domain-based Message Authentication, Reporting and Conformance (DMARC)
64	NA	Generic	Generic	Anti-malware measures	Are email gateways configured to look for potentially malicious links, programs, and block executables?	Yes

Replies to Pre bid Queries for GeM Bid ref. no: GEM/2025/B/5865415 dated 24/01/2025 for Selection of Insurer for Cyber Risk Insurance Policy for a Period of One Year from 31/03/2025 to 30/03/2026 in Canara Bank						
Sl. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Reply
65	NA	Generic	Generic	Anti-malware measures	Is web-based content filtering enforced with restricting access to social media sites, platforms?	Yes
66	NA	Generic	Generic	Anti-malware measures	Are macros disabled by default?	Yes
67	NA	Generic	Generic	Anti-malware measures	Are ransomware specific incident response processes in place? Are ransomware scenarios tested at least annually?	Yes
68	NA	Generic	Generic	Generic	System interconnectivity between the Insured's Parent, non-insured subsidiaries, sister companies & JV entities. If yes, please confirm name of entity, relationship and level of connectivity as per below pointers. By system interconnectivity we mean sharing any of the following: i. Shared Folders ii. Active directory iii. Email Systems iv. Security System v. Network infrastructure vi. Web Domain vii. ERM or CRM type applications (e.g. SAP, Salesforce, etc.) viii. Common Datacenter ix. Common IT team managing multiple IT environment of group companies. x. End user systems xi. Operational technology	All subsidiaries/JV entities have extended their link to our partner zone through private MPLS connectivity.
69	NA	Generic	Generic	Generic	The Policyholder implements the same level of control for each and all the other subsidiaries as declared for the Policyholder at the Parent level.	No subsidiaries are covered under the policy

Replies to Pre bid Queries for GeM Bid ref. no: GEM/2025/B/5865415 dated 24/01/2025 for Selection of Insurer for Cyber Risk Insurance Policy for a Period of One Year from 31/03/2025 to 30/03/2026 in Canara Bank						
Sl. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Reply
70	NA	Generic	Generic	Generic	The Policyholder submits a Remediation Measures Affirmation, confirming that all the remediation measures specified below have been successfully implemented to the satisfaction of the Insurer: i. Implementation of an Attack Surface Management (ASM) solution across all Insured operating companies to ensure critical patches for vulnerabilities with score between 9.0-10 as measured in Common Vulnerability Scoring System (CVSS) and/or those listed on CISA Known Exploited Vulnerabilities Catalog are applied within 72 hours. ii. Multi-factor Authentication controls have been enhanced such that enrolment / reset of MFA token cannot be performed over internet and only one device can be enrolled to generate MFA tokens. iii. Policyholder has engaged a third party to conduct a review of privileged account use across all Companies, shared the results with the Insurer and reduced privileges and/or footprint for those privileged accounts identified within 3 months from inception of the Policy	i. We have in-house vulnerability assessment tools and in-house VA is conducted periodically. Further, we induct Cert-In empanelled external auditors to conduct comprehensive VA&PT twice an year as per our policiy. We have established policies and SOPs that define the TAT for mitigating/remediating the vulnerabilities identified and the same is being followed. ii.We are already aligned with the enhanced feature and are implementing them within our processes. iii.Annual vendor risk assessment is conducted based on the checklist in line with IT Oustsourcing policy, through external auditors.
71	NA	Generic	Generic	Generic	Details for EDR What EDR is in use? Please provide product link + modules implemented What is coverage of EDR (Workstations, Servers, Cloud, etc) Who performs review of EDR logs and at what frequency? Is EDR implemented in block mode with tamperproof installation?	Bank is using Symantec Endpoint Detection & Response Solution .https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-detection-and-response/4-10/what-s-new-in-4-3-v131146855-d38e74614.html Coverage -PCs EDR is intregrated with SIEM and tickets are generated on daily basis. EDR cannot be uninstalled or disabled at endpoint level and is managed centrally.
72	NA	Generic	Generic	Generic	Forensic reports for all ransomware incidents that might have occurred in client's environment in last 18 months	Not applicable (As No ransomware incident/attack during last 18 months)
73	NA	Generic	Generic	Generic	Inventory of External IP(s) of the Insured, including subsidiaries	The bank has above1000* external Ips (* As on 31-01-2025)

Replies to Pre bid Queries for GeM Bid ref. no: GEM/2025/B/5865415 dated 24/01/2025 for Selection of Insurer for Cyber Risk Insurance Policy for a Period of One Year from 31/03/2025 to 30/03/2026 in Canara Bank						
Sl. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Reply
74	NA	Generic	Generic	Generic	Inventory of Domains belonging to the Insured, including subsidiaries	There are approximately 9* domains hosting various underlying sub-domains/applications (* As on 31-01-2025)
75	NA	Generic	Generic	Generic	Copy of Executive Summary of Penetration testing report (provided penetration testing was comprehensive & clean). Definition of clean penetration testing report: i. Test conducted in last 6 months ii. Test conducted by qualified resource iii. Coverage includes of test includes 1. network layer pen test + application layer pen test 2. Network pen test includes all public IP addresses that are accessible over internet (This would include and not limited to below examples) 1. Production systems 2. DR systems 3. Development / Test / UAT / Staging / Other non-production environments 4. Branch IP addresses (if any) iv. Outcome of test confirms: 3. No issues identified with rating of 'Critical' / 'High' 4. Any ports offering remote services without MFA (example RDP) are either be not accessible over internet or MFA is be enabled on them.	Bank is conducting VA&PT on periodic basis though Cert-in Empannelled security auditors. The reports are available and are comprehensive and clean. (Reports cannot be shared as it is confidential)
76	NA	Generic	Generic	Generic	Queries regarding Log4j vulnerabilities. i. What have you done to identify assets that use Log4j in your environment, especially internet-facing ones? ii. What affected systems have you patched so far, and when did you patch them? iii. How are you handling the potential compromise of those systems? iv. What steps have you taken to block Log4Shell attacks, and what extra monitoring, if any, are you doing?	i. All internet facing machines assets have been scanned to check Log4j vulnerabilities. ii.The vulnerabilities have been fixed where ever reported iii.No compromise observed on systems. iv.Blocking policies are implemented and Signatures have been updated in security devices.Also,vulnerability scans are performed to identify such vulnerabilities.



Replies to Pre bid Queries for GeM Bid ref. no: GEM/2025/B/5865415 dated 24/01/2025 for Selection of Insurer for Cyber Risk Insurance Policy for a Period of One Year from 31/03/2025 to 30/03/2026 in Canara Bank						
Sl. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Reply
76	NA	Generic	Generic	Generic	Queries regarding Log4j vulnerabilities. i. What have you done to identify assets that use Log4j in your environment, especially internet-facing ones? ii. What affected systems have you patched so far, and when did you patch them? iii. How are you handling the potential compromise of those systems? iv. What steps have you taken to block Log4Shell attacks, and what extra monitoring, if any, are you doing?	i. All internet facing machines assets have been scanned to check Log4j vulnerabilities. ii.The vulnerabilities have been fixed where ever reported iii.No compromise observed on systems. iv.Blocking policies are implemented and Signatures have been updated in security devices.Also,vulnerability scans are performed to identify such vulnerabilities.
77	NA	Generic	Generic	Generic	Questionnaire	Bidder to refer Annexure -13 of the RFP document
78	NA	Generic	Generic	Generic	Ransomware Supplemental	Bidder to refer Annexure -13 of the RFP document

Date: 11/02/2025
Place: Bengaluru

Deputy General Manager

केनरा बैंक CANARA BANK Tender Processing Section C.P.&V.M. Wing, H.O., Bengaluru - 560 001 सी.पी. एवं वी. एम. विभाग, प्र.का., बेंगलूरु - 560 001