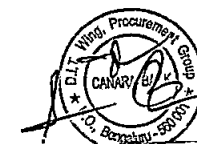


Sl.No.	Bidder Query	Bank's Modified reply
3	Mention the duration in which the company likely to incur a loss of profit after a cyber-attack?	Bank has put in place necessary controls to mitigate all kinds of cyber attacks.
4	Has your organization been compromised in past?	Man-in-the-Middle attack kind of attacks were reported on few ATMs of the Bank in the month of March 2021. Bank has taken adequate steps and implemented TLS 1.2 encryption in all ATMs for encrypted communication between ATM Switch and ATM terminals over and above other controls as per the mandate given by Regulator.
32	Please share information security policy, RTO in case of IT infra failure	Bank is having adequate redundancy setup for Business continuity.
38	Please share Corrective measures taken by the client to prevent occurrence in future.	Bank has implemented TLS 1.2 encryption in all ATMs for encrypted communication between ATM Switch and ATM terminals over and above other controls as per the mandate given by Regulator.
55	Are any data centers / networks being shared between the entities / subsidiaries to be covered / even not covered under the policy please explain in detail?	Subsidiary entities network is not part of Bank's network. Bank's CISO is also Group CISO & Bank's Chief Compliance Officer is also Group Chief Compliance Officer who are overseeing the Information Security and Compliance matters of the Subsidiaries. Adequate measures have been put in place by Subsidairees to safeguard their Infrastructure.
101	Please help with the future plans / improvements / roadmap for cyber security architecture including time frames to implement if any?	Banks is certified with ISO 27001 and all security measures are in place as per the industry best practices.
126	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?	1.Yes 2. Patches are applied on N- 1 basis for all systems. 3.Near 100% 4.Yes 5.Yes
127	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?	1. Backup is in place and enforced. 2,3.Backups are restored and tested at periodical intervals as per industry best practices. 4,5:As per Bank's Backup policy. 6.Yes



Sl.No.	Bidder Query	Bank's Modified reply
128	<p>IRP, BCP, DRP</p> <ol style="list-style-type: none"> 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? <ol style="list-style-type: none"> 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? <ol style="list-style-type: none"> 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? 	<ol style="list-style-type: none"> 1.Yes 2.Yes 3.Yes 4.BCP is ensured to prevent unplanned outages. 5.As per Bank's policy 6.Yes
139	<p>Additional clarifications : -</p> <ol style="list-style-type: none"> 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? 	<ol style="list-style-type: none"> 1,2. Yes 3.Yes 4.Yes
140	<ol style="list-style-type: none"> 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? 	<ol style="list-style-type: none"> 5.yes 6.Yes 7.Yes 8.Yes 9.NA



Sl.No.	Bidder Query	Bank's Modified reply
141	<p>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?</p> <p>11.Are possible Log4j exploitation behaviours (suspicious remote PowerShell execution, obfuscated command/script launched, network traffic connection to C2 server) triaged and remediated immediately?</p> <p>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?</p>	<p>10.Yes 11.No such incident 12.NA</p>
142	<p>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?</p> <p>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?</p>	<p>13.Yes 14.No</p>
144	<p>Does the Applicant have a documented process to respond to phishing campaigns (whether targeted specifically at the Applicant or not)?</p> <p>Yes No</p> <p>If "Yes", please describe the principal steps to respond:</p>	<p>Yes. Actions are taken as per incident response plan of the Bank.</p>
155	<p>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)"</p> <p>Please enter an integer: Additional commentary on the number of privileged accounts:</p>	<p>In terms of Bank's policy.</p>
157	<p>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)?</p> <p>There is no defined policy for when patches must be deployed.</p> <p>Within 24 hours. 24-72 hours. 3-7 days. > 7 days.</p> <p>Additional commentary on target times for patching: Critical patches/security patches are deployed as and when required</p>	<p>Patches are applied on N- 1 basis for all systems.</p>



Sl.No.	Bidder Query	Bank's Modified reply
158	<p>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:</p>	Near 100% as per industry standards.
187	<p>Steps taken by the company to prevent potential Data Breach incidents due to all/most employees working from home?</p>	<p>All necessary controls have been implemented including but not limited to as mentioned below to prevent any data breach incidents: 1. Strict access controls 2. Continuous monitoring of incoming/outgoing network traffic 3.Tier 3 architecture for webfacing systems. 4.VLAN segregation 5.24x7 Monitoring through SOC solutions 6.Deception solutions 7.Data in transit and Data at rest are implemented. etc. 8. Infrastructure audit is conducted at regular intervals by third party auditors as per requirement.</p>
199	<p>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.</p>	<p>1.Yes 2.Procurement is as per the technical specification requirements which covers security aspects also. 3.No</p>
200	<p>Were there any critical findings in the VAPT testing? Have all the findings been implemented? How frequently is VAPT conducted?</p>	<p>VAPT is conducted as per the Bank's policy inline with Regulator and industry best practices. Immediate remediation of vulnerabilities is taken care.</p>
207	<p>Please provide BCP copy</p>	<p>BCP is internal classified document. Details will be shared with the selected bidder.</p>
208	<p>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?</p>	<p>Process elements including but not limited to in BCP framework are a.Business Impact Analysis b.Risk assessment c.Monitoring of risks d.Dr Drills etc. 2. As per Bank's policy 3. Bank has put in place necessary controls to mitigate all kinds of cyber events. 4.As per Bank's policy</p>
210	<p>What's (roughly) the ratio commercial vs open-source software/applications in your company?</p>	<p>Only licensed software is used.</p>
211	<p>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?</p>	<p>Bank is having Tier III Datacenters (DC&DR) and Data processing is centralised.</p>



Corrigendum to 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.	Bidder Query	Bank's Modified reply
212	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	1. Please refer to Financial results data in Bank's Website 2. Please refer to Bank's data in RBI Website 3. Bank's IT Infra is PCI DSS compliant as mandated by RBI.
213	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?	Yes
214	Are any servers / desktops accessible via remote connectivity i.e remote desktop, team viewer, etc.? If yes. How is access to those servers protected?	All required control measures are put in place for accessing Bank's systems. The controls are audited and reviewed by third party auditors also.
215	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	a. Yes b. Yes c. All systems & controls are in place to ensure business continuity.
216	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.	Security Standard in each location is very high
217	Operational recovery procedure: description of the existing back-up procedures and capabilities?	Backups are taken as per extant policy of the as ^{part} of BCP.
218	Existing patching process and procedure in case patching process for IT /OT assets fails? Please describe the rollback procedure in the event a failure happens once implemented into production	Patching process is as per Bank's policy/SOP.
224	Please help with the future plans/improvements for cyber security architecture including time frames to implement any ?	Banks is certified with ISO 27001 and all security measures are in place as per the industry best practices.
226	Microsoft Questionnaire Has Insured/Applicant completed an impact/risk assessment of this event? Yes No Additional commentary:	Yes for Microsoft Exchange On-premise product being used in the Bank.
227	In connection with the event, does the Insured/Applicant use any externally facing version of the product? Yes No Additional commentary:	No
235	Limitation & Control of Network Ports a) RDP port has been disabled/closed b) SMB port has been disabled/closed	All industry best practices are being followed. All mitigation controls are put in place as per the VAPT assessments through third party auditors.



Sl. No.	Bidder Query	Bank's Modified reply
243	Has Insured/Applicant completed an impact/risk assessment of the following events noted below? 1. Apache Log4j vulnerability (CISA Emergency Directive 22-02) <input type="checkbox"/> YES <input type="checkbox"/> NO 2. Microsoft On Premise Exchange Server (CISA Emergency Directive 21-02 issued 3/3/21) <input type="checkbox"/> YES <input type="checkbox"/> NO 3. Ivanti Pulse Connect Secure Products (CISA Emergency Directive 21-03 issued 4/20/21) <input type="checkbox"/> YES <input type="checkbox"/> NO 4. Kaseya On Premise Server (CISA-FBI Guidance for MSPs and their Customers issued 7/4/21) <input type="checkbox"/> YES <input type="checkbox"/> NO 5. Microsoft Window Print Spooler (CISA Emergency Directive 21-04 issued 7/13/21) <input type="checkbox"/> YES <input type="checkbox"/> NO	1. Yes 2. Yes 3. Yes 4. Yes 5. Yes
244	Does the Insured/Applicant use any of the impacted software code, products or applications identified in any of these events? (check all that apply) <input type="checkbox"/> Apache Log4j <input type="checkbox"/> Microsoft On Premise Exchange Server <input type="checkbox"/> Ivanti Pulse Connect Secure <input type="checkbox"/> Kaseya On Premise VSA Server <input type="checkbox"/> Enabled Microsoft Windows Print Spooler	<input type="checkbox"/> Apache Log4j <input type="checkbox"/> Microsoft On Premise Exchange Server
245	Have all CVE's assigned to those vulnerabilities been remediated? 1. Apache Log4j (CISA Emergency Directive 22-02) <input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A 2. Microsoft On Premise Exchange Server (CISA Emergency Directive 21-02 issued 3/3/21) <input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A 3. Ivanti Pulse Connect Secure Products (CISA Emergency Directive 21-03 issued 4/20/21) <input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A 4. Kaseya On Premise Server (CISA-FBI Guidance for MSPs and their Customers issued 7/4/21) <input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A 5. Microsoft Window Print Spooler (CISA Emergency Directive 21-04 issued 7/13/21) <input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A	Yes remediated in all applicable solutions.
246	Has Insured/Applicant initiated any forensic analysis to identify any IOC (Indicator of Compromise) resulting from the identified security flaw(s)? <input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A	No such incident
247	Were any IOC's identified during the forensic analysis on any of the following products? (check only if identified) <input type="checkbox"/> Apache Log4j <input type="checkbox"/> Microsoft On Premise Exchange Server <input type="checkbox"/> Ivanti Pulse Connect Secure <input type="checkbox"/> Kaseya On Premise VSA Server <input type="checkbox"/> Enabled Microsoft Windows Print Spooler	No such incident

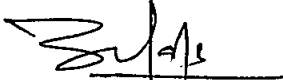


Sl.No.	Bidder Query	Bank's Modified reply
248	<p>If any IOC's were identified has the Insured/Applicant remediated and removed any identified Malware in the Insured/Applicant's computer system for the following products? Apache Log4j vulnerability (CISA Emergency Directive 22-02) <input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A N/A Microsoft On Premise Exchange Server (CISA Emergency Directive 21-02 issued 3/3/21) <input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A Ivanti Pulse Connect Secure Products (CISA Emergency Directive 21-03 issued 4/20/21) <input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A Kaseya On Premise Server (CISA-FBI Guidance for MSPs and their Customers issued 7/4/21) <input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A Microsoft Window Print Spooler (CISA Emergency Directive 21-04 issued 7/13/21) <input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A</p>	No such incident
249	<p>Does any of the Insured/Applicant's critical vendors use any of the affected products or applications identified in the events list above? <input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> Unknown</p>	Yes as applicable. Remediation actions are taken.
250	<p>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) <input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A Microsoft On Premise Exchange Server (CISA Emergency Directive 21-02 issued 3/3/21) <input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A Ivanti Pulse Connect Secure Products (CISA Emergency Directive 21-03 issued 4/20/21) <input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A Kaseya On Premise Server (CISA-FBI Guidance for MSPs and their Customers issued 7/4/21) <input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A Microsoft Window Print Spooler (CISA Emergency Directive 21-04 issued 7/13/21) <input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A</p>	We are not hosting any application in vendor environment.



Sl.No.	Bidder Query	Bank's Modified reply
251	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) <input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A Microsoft On Premise Exchange Server (CISA Emergency Directive 21-02 issued 3/3/21) <input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A Ivanti Pulse Connect Secure Products (CISA Emergency Directive 21-03 issued 4/20/21) <input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A Kaseya On Premise Server (CISA-FBI Guidance for MSPs and their Customers issued 7/4/21) <input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A Microsoft Window Print Spooler (CISA Emergency Directive 21-04 issued 7/13/21) <input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A	No
252	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):"	As Bank's operational requirement.

Date: 04/02/2022
Place: Bengaluru


Deputy General Manager
