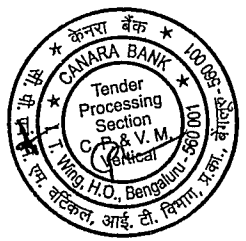
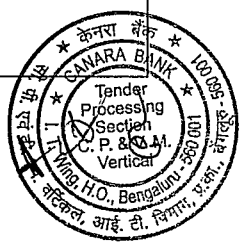
Sl. No.	Section / Annexure / Appendix	RFP Clause	Bidders Querry	Bank Response
1	NA	NA	Does the company have Board approved Information Security & privacy policy and it is communicated to all stakeholders? Please confirm which option is applicable Ø No information policy is present Ø ISP is present but not approved by board Ø ISP is present & approved by board Ø Approved Policy is in place but not communicated to all stakeholders Ø Policy is in place and communicated to all stakeholders\	ISP is present & approved by board Policy is in place and communicated to all stakeholders
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? Please confirm which option is applicable Ø No, Incident Response, Business Continuity plan, Disaster recovery plan are not present Ø IR/BC/DR is present but not approved by board Ø IR/BC/DR is present & approved by board Ø Approved Disaster recovery plan, Business Continuity plan are present but not reviewed Annually Ø Approved Disaster recovery plan, Business Continuity plan are present and are reviewed Annually	Yes.Approved Disaster recovery plan, Business Continuity plan are present and are reviewed Annually.
3	NA	NA	Mention the duration in which the company likely to incur a loss of profit after a cyber-attack? Please confirm which option is applicable Ø 1-12 Hours Ø 12-24 Hours Ø 24 to 36 Hours Ø 36 to 48 Hours Ø 48 Hours and above	Varies according to the type of attack
4			Has your organization been compromised in past?	No
5	NA	NA	Which are the information security certification hold by your organization? Please confirm which option is applicable Ø ISO 27001 Ø PCI DSS Ø ISO 27004 Ø ISO 22301 Ø ISO 27017 Ø SOC2 Ø None Ø Please mention if any other	ISO 27001 PCI DSS
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?	Varies according to the type of attack

Sl. No.	Section / Annexure / Appendix	RFP Clause	Bidders Querry	Bank Response
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? Please confirm which option is applicable Ø Data is shared but Audit is never conducted Ø Review/Audit is done only at the time of on boarding Ø Audit/Review is conducted at least once in two years Ø Audit/Review is conducted at least once a year Ø Not applicable as company do not share critical info with any other third party	Audit/Review is conducted at least once a year
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?	No
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) Please confirm which option is applicable only conducted at the time of joining No Cyber security trainings are conducted Conducted once in a year for all employees Conducted Twice in a year for all employees Conducted More than 2 times in a year	Conducted on a regular basis
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? Please confirm which option is applicable No Security Audit Log Report is generated At least monthly At least Fortnightly At least weekly Automated continuous review is schedule	Automated continuous review is scheduled
13	NA	NA	Are only fully supported/updated web browsers and email clients allowed to execute in the organization?	Yes

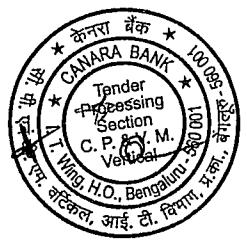
Sl. No.	Section / Annexure / Appendix	RFP Clause	Bidders Querry	Bank Response
14	NA	NA	Is secure configuration is used for all softwares and hardware (Mobile devices, Laptop, Workstations and servers) including network devices (firewall, router and switch)?	Yes
15	NA	NA	How often assessment programs run to determine wheather all systems' softwares & security patches are updated?(including remote access connection) Please confirm which option is applicable No assessment programs are scheduled once in a Fortnight once in a week once in a day Continuous assessment Program is scheduled	As per the approved policy, patches are updated on regular basis
16	NA	NA	Does company have Anti-virus & Firewall installed on computer system? If yes, What is the frequency for updating this? Please confirm which option is applicable Anti virus & Firewall are not installed Updated At least Within a month Updated Within A fortnight Updated Within a Week Updated daily	Yes.Updated daily
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? Please confirm which option is applicable No Network Access control Network Access control for Authenticated Devices only Network Access control for Authenticated Software only Network Access control for both Authenticated Software and Devices	Network Access control for both Authenticated Software and Devices
20	NA	NA	How often all the Ports are scanned against all critical servers for to & fro data movement? Please confirm which option is applicable No Scans are performed Monthly Scans Weekly Scans Daily Scans Continuous scanning of key servers	Monthly Scans



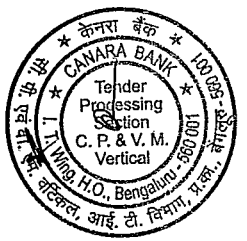
Sl. No.	Section / Annexure / Appendix	RFP Clause	Bidders Querry	Bank Response
21	NA	NA	Does the company have checks in place to identify and detect network security weakness? (internal/External Vulnerability assessment)	Yes
22	NA	NA	Does the organization have End point Solutions in Place ?	Yes
23	NA	NA	Does the Insured have a Behavorial based end point?	Behavioural based AV is in place
24	NA	NA	Any external or internal penetration tests are conducted to identify vulnerabilities or attack vectors? If yes, What is the frequency of penetration tests Please confirm which option is applicable Never Once in two years Yearly Half Yearly At least Quarterly	Half Yearly
25	NA	NA	In case of cyber attack, which multilayer boundary defence are in place to filter inbound and outbound traffic (including business partner network)? Multiple Choice Please confirm which option is applicable Ø None Ø Stateful firewall/Proxy firewall (Basic) Ø Static packet filter Ø IDS and IPS Ø VPN device Ø NGF(Next gen firewall)/web application firelwall	Bank is ISO 27001:2022 and PCI DSS certifications. Multiple layers of boundary defences are in place. Specifics cannot be disclosed since confidential
26	NA	NA	Which type of data organization collect, store & process? (Multiple Choice) Please confirm which option is applicable Financial/Credit/Payment Card Data Medical/Healthcare Personal Identity Data Business(corporate Info) None of the above	Financial/Credit/Payment Card Data Personal Identity Data
27	NA	NA	What is the frequency of Data Back Up(Operating System, Application Software and Data)? Please confirm which option is applicable Never Monthly Fortnightly Weekly At least twice in a Week	Data is being backed up on regular intervals as per approved backup guidelines.



Sl. No.	Section / Annexure / Appendix	RFP Clause	Bidders Querry	Bank Response
28	NA	NA	Has your organisation undertaken a Phishing Campaign on Peroidic basis ?	Yes
29	NA	NA	What percentage of your employees fell for the trap in your Phishing Campaign? Please confirm which option is applicable Ø Less than 10% Ø 10% - 20% Ø 21% - 30% Ø Above 30%	Less than 10% (In last exercise, it was 1.46%)
30	NA	NA	How many times data restoration process is verified to ensure back up data is properly working? Please confirm which option is applicable Never Quarterly Monthly Fortnightly Weekly	As per approved guidelines of the bank
31	NA	NA	Is data in stored form(On Cloud, Servers,Laptops,flash drives, back up tapes) or in transit form, encrypted using strong encryption technologies? Please confirm which option is applicable No encryption technology is used Data in stored form only is encrypted Data in stored form and in transit form is encrypted	Data in stored form and in transit form is encrypted
32	NA	NA	Are data access restrictions inforced on the basis of specific role rights ?	Yes. RBAC is in place
33	NA	NA	How many times Admin access rights are reviewed to ensure only that only administrative functions (Non-Internet Connection based) are performed on those systems? Please confirm which option is applicable Ø No review is performed on administrative account Ø Yearly Ø Quarterly Ø Monthly Ø Fortnightly	Monthly

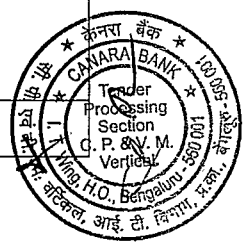


Sl. No.	Section / Annexure / Appendix	RFP Clause	Bidders Querry	Bank Response
34	NA	NA	Which user access management methods are being used in your organization? (Multiple Choice) Please confirm which option is applicable Ø Disable account that is not associated with any business owner & process Ø Revoking system access immediately after termination Ø Strong Password policy with unique, complex & with expiration date Ø Screen locks on unattended systems Ø Lockouts after a set number of failed login attempts Ø Clear Desktop Policy	All the mentioned options are in place along with Multi factor Authentication
35	NA	NA	Does company have security controls in place to authenticate all user(including remote user and wireless area) before being allowed to connect to internal network and computer system?	Yes
36	NA	NA	Please share information security policy, RTO in case of IT infra failure	Policy is confidential.
37	NA	NA	Is SOC empowered to perform continuous data monitoring?	Yes
38	NA	NA	Which EDR solution is installed on all end points?	EDR solution is installed on all end points, specifics are confidential.
39	NA	NA	Is financial messaging systems (NIFT/SWIFT) is audited regularly?	Yes. SWIFT audit is conducted regularly.
40	NA	NA	Please share claim details under existing Cyber Policy ending on 30th March 2024	No claims are raised for the existing period
41	NA	NA	Please confirm Current status of claim along with Admissibility status along with Claim Reserve Created by Insurer	NA
42	NA	NA	Please share Corrective measures taken by the client to prevent occurence in future.	NA
43	NA	NA	Please share Policy Copy for Policy Period from 31st March 2023 to 30th March 2024	We cannot share current policy copy. The draft policy is shared as per Corigendum-1.
44	NA	NA	Whether any Claim has been reported under the said Policy for the past three years and if so, quantum of claim and the claim status as on date.	No claim since 31-03-2021



Sl. No.	Section / Annexure / Appendix	RFP Clause	Bidders Querry	Bank Response
45	NA	NA	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.
46	NA	NA	Please list all the cyber 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.) or please share IT org chart.	Information Security functions include: 1. 24*7 monitoring in SOC 2. Incident response and management 3. Periodic internal VA and external VAPT 4. Red Team 5. DAST 6. Threat Hunting 8. Periodic Table Top Exercise & Drill 9. Periodic Phishing Simulation Exercise 10. Cyber Security Awareness 11. Action on Threat Intel Feeds received from CSITE, Cert-In, NCIIPC etc. 12. Regulatory Compliance
47	NA	NA	Do you have a process of real time monitoring for Domain admin accounts? Kindly elaborate?	Yes. Alerts are created and appropriate actionsare being taken.
48	NA	NA	Please describe your current status with regards to Zero trust architecture for your network? What are the ongoing projects towards ZTA?	Bank has adopted Zero trust architecture. Details are confidential.
49	NA	NA	Kindly describe your current cyber security monitoring setup. Please explain by way of an example, how day-to-day operations of your cyber security monitoring setup takes place i.e. - typical process when a alert is generated to resolution and updating of use cases? - Have you established an escalation procedure for information security incidents?	The organisation have a dedicated Security operation centre (SOC) which operates 24*7*365 at inhouse takes care of implementation, operations & monitoring, consisting of SOC manager, analysts and incident handlers. Alert generated is assigned to corresponding stakeholder and closure is ensured within TAT. Use cases and rules are updated regularly. Escalation procedures are established.
50	NA	NA	Are all your Critical services on Active- Active setup?	Yes
51	NA	NA	Please describe the scope of your BCP testing. Was it Table-top or functional?	Functional
52	NA	NA	Operational recovery procedure: description of the existing back-up procedures and capabilities?	Bank is having approved backup guidelines. Backups are taken according to the prescribed guidelines.
53	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?	Bank has defined policy for patching and roll back process.
54	NA	NA	What redundancies are leveraged in the design of your infrastructure ? (E.g., automatic failover logic, multiple processors, redundant I/O modules, Dual trinked networks)	Auto failover logic
55	NA	NA	Do you test updates and upgrades of firmware, software, web-applications and products of your systems before deployment?	Bank follows defined UAT and release management process
56	NA	NA	What kind of redundancies do you leverage for your mission critical systems? Are you on a hot or warm site standby?	We are on Active-active and Hot standby mode.
57	NA	NA	What kind of Recovery Time Objectives (RTO) do you have for your mission critical systems and are these time objectives tested at least annually?	RTO is defined for each critical systems and are tested periodically as part of DR Drill.

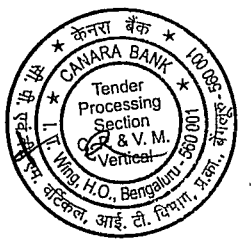
Sl. No.	Section / Annexure / Appendix	RFP Clause	Bidders Querry	Bank Response
58	NA	NA	Please let us know how do you arrive at your RTO and RPO	RTO and RPO is defined on BIA of individual applications based on its complexity, inter-dependency, functioning and criticality.
59	NA	NA	Are in house developed 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
60	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. Details are confidential.
61	NA	NA	What redundancies do you leverage in the design of your infrastructure? (E.g. automatic failover logic, multiple processors, redundant I/O modules, dual-trunked networks)	Auto fail over logic
62	NA	NA	In the absence of a fully redundant primary control system, have you implemented a secondary control system as backup?	Yes
63	NA	NA	Do you have Segregation of Network based on Business Function to avoid lateral spread?	Yes
64	NA	NA	Please let us know how a typical BCP testing looks like in terms of Role played by different team and the process	BCP Review is conducted on regular intervals. Once approval is received from competent authorities, Tabletop Exercise will start by involving all the vendors, functional and technical groups. Then DR drill is conducted on approved date. Once all the applications involved starts working from standby , application team verifies all functions. Once verified, application works from standby side over a period of time. Post-Drill Actionable Measures is implemented to avoid reccurance. Also, drill Report is prepared and submitted to higher officials.
65	NA	NA	Do you test security functionality during the development lifecycle of information systems incl. IT security updates? If the response is no: request you to kindly share some more details on this aspect?	Yes
66	NA	NA	Please provide organizational structure of the company (subsidiaries and other entities required to be covered - if any)	Head office ;Circle Office, supporting Regional Offices and Branches. No subsidiaries are covered.
67	NA	NA	We would need to understand the current structure of the IT-Information security team in terms of Roles, function and reporting and Strength (no of people)	Information Security Team is reporting to CISO. Team size of appprox. 70* members are there consisting of SOC manager, analysts and incident handlers, Cyber security, Network Security, Server Security and endpoint security. (* As on 31-01-2024)
68	NA	NA	Please let us know if the IT security principles/policies/infrastructure and the team managing the function is centralized or decentralized. This needs to be in context all the entities (subsidiaries and manufacturing locations and offices including global entities if any) proposed to be covered under the policy	It is being handled centrally.
69	NA	NA	Brief description on nature of operations being done from new branch at GIFT City	Branch is dealing with overseas operations inland.



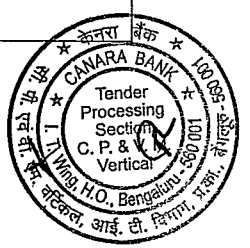
Sl. No.	Section / Annexure / Appendix	RFP Clause	Bidders Querry	Bank Response
70	NA	NA	Details and nature of the data stored & No. of Records: - PII - PCI - PHI	PII and PCI
71	NA	NA	Below documents would be required - ISO 27001 - PCI DSS certificates	We are certified and the documents are in place
72	NA	NA	Last 3 years premium & claim statistics	No claim since 31-03-2021.
73	NA	NA	Brief description of the claim/notifications, if any	NA
74	NA	NA	Please share the draft policy wordings for this year's renewal	The draft policy is shared as per Corigendum-1.
75	NA	NA	List of Inventory of External IP(s) of the Insured, including subsidiaries	We have more than 1000* IP addresses. (* As on 31-01-2024)
76	NA	NA	List of Domains belonging to the Insured, including subsidiaries	There are approximately 8* domains hosting various underlying sub-domains/applications (* As on 31-01-2024)
77	NA	NA	Queries regarding Log4j vulnerabilities: 1. What action is taken to identify assets that use Log4j in your environment, especially internet-facing ones? 2. What affected systems have been patched so far, and when were they patched? 3. How is the potential compromise of those systems handled? 4. What steps have been taken to block Log4Shell attacks, and what extra monitoring, if any, is being done?	-All internet facing machines assets have been scanned to check Log4j vulnerabilities. -The vulnerabilities have been fixed where ever reported and no compromise observed on systems. -Blocking policies are implemented. -Signatures have been updated in security devices. -Also,vulnerability scans are performed to identify such vulnerabilities.
78	NA	NA	In view of recent UCO bank IMPS fraud, do the IT vendors of Canara Bank have any separate PI policies in place?	Not available
79	NA	NA	Please share expiring policy copy.	We cannot share current policy copy. The draft policy is shared as per Corigendum-1.
80	NA	NA	Kindly share claims History under the policy for last 5 years.	No claim since 31-03-2021. However, during 2020-21 FY, a Cyber Fraud was intimated by the Bank in the month of March 2021.Perpetrators executed a man-in-the-middle attack, manipulating transactions to force the ATM to dispense cash. While the bank managed to recover a portion of the lost funds, it was within the deductible, resulting in a claim status of Nil.
81	NA	NA	Would the Insured please confirm they do not have any exposure to: 1. CVE-2023- 34362 zero day vulnerability recently identified within the MOVE-it software provided by Progress Software & 2. Citrix Bleed NEW Zero Day Vulnerability CVE 2023- 4966	No exposure to the mentioned vulnerabilities
82			What is your approach to managing zero-day vulnerabilities? Are you able to escalate patching in these circumstances?	Zero day vulnerabilities are handled by Antivirus, Sandboxing and Virtual Patching.
83			List of open claims/incidence if any. If yes, please share details on incidence and corrective measures undertaken to mitigate & minimize the risk.	No open claims

Sl. No.	Section / Annexure / Appendix	RFP Clause	Bidders Querry	Bank Response
84			Are each of the branches and ATM's segregated from one another and have maintained on their own network infrastructure? i.e. if there is downtime at one branch, will this impact the rest of the business or can they continue to operate as normal?	Branches and ATMs are segregated as separate VLANs. Also, downtime at one branch will not affect the rest of the business
85	NA	NA	Do they have BBB/ECC policy. If yes, please share details (Limits) since Crime covers(If any) will operate in excess of these.	We have Banker's indemnity policy in place
86	NA	NA	Total no of PII stored/handled? Maximum amount of PII in a single DB?	PIIs such are aadhar, DOB, PAN etc. are stored. Other details are confidential.
87	NA	NA	Access controls to the data? Is this limited to a select number of users? Does this require MFA?	Access controls including RBAC,MFA etc. are in place
88	NA	NA	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 (N-1) basis. Monitoring of servers/network in real time is being done. Vulnerability scanning tools are available and the details cannot be disclosed.
89	NA	NA	What logging capabilities are available to you? and how long do you retain logs for?	Log retention is as per our approved policy.
90	NA	NA	Please share draft policy wordings	The draft policy is shared as per Corigendum-1.
91	NA	NA	1. Does the Company have various subsidiaries/Associate/Group companies to be covered, do let us know if the IT security policy and measures are centralized for them and the information shared is applicable to those entities as well. Also let us know who is responsible for management of Information/Network securities for these entities. a) If its not centralized, do let us know how are they managed b) Who manages active directory environment c) Is network of the proposer company interconnected with other entities to be covered, If yes, we need to know what systems/data are exposed and what controls are in place to minimize infection/hacking etc d) Is the information and risk assessment questionnaire true for all the entities to be covered	No subsidiaries are covered in the scope of this policy.
92	NA	NA	2. Please let us know a) Current IT security team functions and role including the basic functions which are being performed currently including the structure, reporting and responsibilities CISO (Chief Information Security Officer), CTO (Chief Technology Officer), CRO (Chief Risk Officer), CSO (Chief Security Officer), etc b) Inhouse and Outsourced security functions (e.g Threat Intelligence, NOC, SOC and Incident Response, ATM Security)	a)Information Security functions include: 1. 24*7 monitoring in SOC 2. Incident response and management 3. Periodic internal VA and external VAPT 4. Red Team 5. DAST 6. Threat Hunting 8. Periodic Table Top Exercise & Drill 9. Periodic Phishing Simulation Exercise 10. Cyber Security Awareness 11. Action on Threat Intel Feeds received from CSITE, Cert-In, NCIIPC etc. 12. Regulatory Compliance

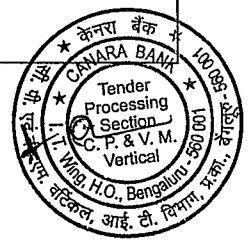
Sl. No.	Section / Annexure / Appendix	RFP Clause	Bidders Querry	Bank Response
93	NA	NA	3. Confirm on; No of a) Employees: _____ b) Branches: ____ c) ATM: _____ d) No of Customers: Please state the (estimated) number of individual IT devices deployed Server a) On Premises b) On Cloud Desktops/ Laptops/ Mobile devices/Portable Media Network Diagram (if available)	a) Employees: 83824* b) Branches: 9585* c) ATM:12120* d) No of Customers: More than 11* Crore (* As on 31-01-2024) Servers are deployed on premises as well as cloud. (Network diagram is available and confidential)
94	NA	NA	Confirm on Bank's compliance with "Cyber Security Framework in Banks" circular guidelines of RBI, whether (Fully/Partially/Not compliant) if not compliant let us know the Roadmap (C-SOC,review of network,Cyber Crisis Management Plan (CCMP),Review BCP/DR program,Conduct Cyber Security Awareness and Training sessions...etc)	Yes. Fully compliant.
95	NA	NA	Do you provide training to employees on Information security awareness. Are there any other measures to manage people side of Infosec risk? (eg. Phishing Compagin/ url filtering/web-based content filtering)	Yes. Phishing campaign, whitelisting, content filtering etc. are in place
96	NA	NA	6. Does the Bank have a) Board approved Information Security & privacy policy and is it communicated to all stakeholders? b) Business Continuity Plan (BCP)/Incident Response Plan (IRP)/Disaster Recovery (DR) Plan c) How often above plans tested and when these plans are last reviewed	a)Yes b)Yes c)Plans are tested as per approved framework and the review is annually
97	NA	NA	7. Network segregation a) Please Confirm on Network segregation (VLAN, Micro, DMZ - segregation of ATM, SWIFT, CBS etc. networks and production and test network) b) Please let us know if there is segregation based on geographies and business divisions, branches to avoid any lateral spread of malware	a)Yes b)Yes



Sl. No.	Section / Annexure / Appendix	RFP Clause	Bidders Querry	Bank Response
98	NA	NA	8. BCP and DR: a) Does the BCP plan include impact of a cyber incidence on Business Operation b) Does the BCP plan has defined BIA and RTO for all critical operations c) What is the maximum acceptable outage or also Known as RTO (Recovery Time Objective) for Critical system and RPO (recovery point objective) d) Frequency of IT DR drills e) Confirm on testing of BCP under different scenarios for all possible types of contingencies (i.e. People, Processes and Resources (including Technology). f) What type of DR site/strategy you have i) Cold Site, Warm Site; Hot Site : _____ ii) Active - Passive (Cold/Warm); Active-Active : _____ g) Does the Company have DR Site to continue business operation in the event of disaster h) What redundancies do you leverage in the design of your infrastructure? (E.g, automatic failover logic, multiple processors)	a)Yes b)Yes c)RTO and RPO is defined for each application in the approved BCP framework. d)As per defined policy e)According to BCP framework f)i)Hot ii)Active-Active g)Yes h)Auto fail over
99	NA	NA	9. Confirm on, a) Are firewalls in place at all external connection points? b) Do you review firewall rules, configurations and settings on at least a quarterly basis?	a)Yes b)Yes
100	NA	NA	10. Let us know VAPT Scope (Web,Mobile,IT Infra/Network/API) and Frequency (quarterly/half yearly/Annually) and whether finding in last VAPT has patched if not please provide roadmap	VAPT is conducted for all bank assets incl. Web,Mobile,Server/Network/API periodically according to the policy. All the findings are mitigated.
101	NA	NA	11. Vendor Management a) A maintenance and support contract with all vendors for the systems which is reviewed annually. b) The contract with vendors captures the escalation matrix of vendors which is reviewed annually. c) A documented Third party security policy to ensure the implementation security controls with respect to the services provided by the Third Party. d) Document the changes in the services provided by the third party in the maintenance and support contract. e) Perform risk assessment whenever there is change in the service provided by the third party and appropriate actions are taken for the closure of identified risks. f) Enforced appropriate risk-based multifactor authentication (MFA). g) Access management (provision/modification /revocation).	Cotrols are in place according to the SLA executed and approved policy of the Bank.



Sl. No.	Section / Annexure / Appendix	RFP Clause	Bidders Querry	Bank Response
102	NA	NA	12. Cloud Security a) Has the cloud service undergone any third party cloud security assurance or certification (example: ISO/IEC 27001/27002:2013, ISO 27018, IRAP, SOC 2 etc.)? (Cloud Security Certification) b) Is your cloud service PCI Certified? (Cloud Security Certification) c) Do you use an automated/Manual source code analysis tool to detect security defects in code prior to production? (Application & Interface Security) d) Multi-Factor Authentication enabled for the root account e) Ensure S3 buckets are not publicly accessible (publicly read or write) - f) Continuously inspect and monitor S3 buckets (eg Amazon CloudWatch metrics) g) Integration of cloud log with SIEM with 24*7 monitoring h) Other measures from Cloud security perspective	a)Yes b)Yes c)Yes d)Yes e)Not applicable f)Not applicable g)Yes h)Defenese in depth strategy is followed during implementation
103	NA	NA	13. How Client monitor the network and identify security events? Does 24*7 SOC functionality is available? Whether its outsourced. If this functionality not available then how Insured manage this function	Yes. 24*7 SOC monitoring is in place which is In house.
104	NA	NA	14. Does Malware protection configured have heuristic and behavioural based detection in addition to traditional signature-based detection	Yes
105	NA	NA	Does the organization ensure that any Firewall, Router or Switch deviations from the standard configurations are documented and approved?	Yes
106	NA	NA	16. Email security A) 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) B) What Email Security Solution (Vendor) do you use ? C) Are email gateways configured to look for potentially malicious links, programs, and block executables?	Yes
107	NA	NA	17. What Endpoint Security Technology do you have in place? a) Standard Anti-virus [McAfee MVISION/Symantec/Microsoft Defender/Webroot Endpoint Security...etc] b) Next-Gen Anti-virus [CrowdStrike Falcon Protect/SentinelOne Singularity Core/Sophos Intercept X Advanced..etc] c) Endpoint Detection & Response [CrowdStrike Falcon Insight/SentinelOne Singularity Complete/Sophos Intercept X Advanced with XDR/FireEye Endpoint Security/Microsoft Defender for Endpoint..etc] d) Other endpoint security technology _____	Endpoint Detection & Response



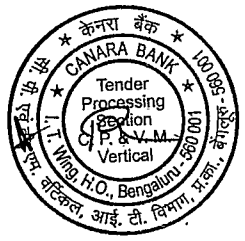
<table>
<tr><th>Sl. No.</th><th>Section / Annexure / Appendix</th><th>RFP Clause</th><th>Bidders Querry</th><th>Bank Response</th></tr>
<tr><td>108</td><td>NA</td><td>NA</td><td>18. Please let us know the details of and the scope of
a) EDR solution 100% i.e. does it include all endpoints, network,Servers, Infrastructure, cloud etc.? Or
b) XDR solution 100% i.e does it include all endpoints, network, Servers, Infrastructure, cloud etc.?</td><td>EDR solution includes all end points. Servers are protected by a different AV solution</td></tr>
<tr><td>109</td><td>NA</td><td>NA</td><td>19. Please let us know the type of third-party Confidential data handled, stored by you and What measures like hashing, anonymising etc is being used to secure data
<table>
<tr><th></th><th>Type of Record</th><th>Whether collect, store, process and/or transmit</th><th>Whether Encrypted</th><th>Approx. Number</th></tr>
<tr><td>a</td><td>Personally Identifiable Information (PII)</td><td>Yes/No</td><td>Yes/No</td><td></td></tr>
<tr><td>B</td><td>Payment Card Information (PCI)</td><td></td><td></td><td></td></tr>
<tr><td>C</td><td>Protectable Health Information (PHI)</td><td></td><td></td><td></td></tr>
<tr><td>D</td><td>Intellectual property (IP)</td><td></td><td></td><td></td></tr>
<tr><td>e</td><td>Other (Please specify)</td><td></td><td></td><td></td></tr>
</table></td><td>Confidential information.

All sensitive data are masked</td></tr>
<tr><td>110</td><td>NA</td><td>NA</td><td>20. Please confirm that all necessary IT security measures including VPN, MFA etc.. are implemented for the remote connections
<table>
<tr><th>Remote Connectivity Type</th><th>MFA in Place? (Yes / No)</th><th>What is 2nd factor in use? (e.g OTP, Call and Authenticator)</th></tr>
<tr><td>VPN</td><td></td><td></td></tr>
<tr><td>VDI</td><td></td><td></td></tr>
<tr><td>Email over Internet</td><td></td><td></td></tr>
<tr><td>Infrastructure hosted in Cloud</td><td></td><td></td></tr>
<tr><td>Any other please provide details (example: RDP; VNC; SSH; AnyDesk; TeamViewer; etc)</td><td></td><td></td></tr>
</table>
a) Confirm on No remote connectivity solution exposed to internet without MFA
b) Confirm on Remote Desktop Protocol (RDP) is disabled or it must be accessed from behind a firewall, through a VPN configured for network-level authentication, and/or the IP addresses of all authorized connections are whitelisted.</td><td>Yes
We use MFA for remote connections.

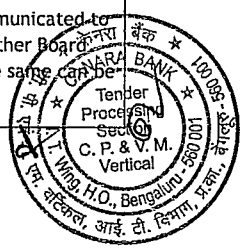
a)Nil
b)RDP is disabled</td></tr>
<tr><td>111</td><td>NA</td><td>NA</td><td>Does the Bank have written patching policy in place with explicit mention to Critical, Important and normal patches with timelines for their implementation, Does the patching process manual or with Automated tool</td><td>Yes. Patching is automated.</td></tr>
<tr><td>112</td><td>NA</td><td>NA</td><td>For the current legacy systems in your network
a) Please let us know the compensatory control in place to avoid misuse of any vulnerability
b) Please let us know number of such systems and timelines to phase them out completely</td><td>Legacy systems are not used</td></tr>
</table>

<table>
<tr><th>Sl. No.</th><th>Section / Annexure / Appendix</th><th>RFP Clause</th><th>Bidders Querry</th><th>Bank Response</th></tr>
<tr><td>113</td><td>NA</td><td>NA</td><td>Confirm whether Data Loss Prevention solution is present (DLP) and scope of DPL - (Network/Endpoint/Email/Cloud)</td><td>Yes. In network, email and endpoints</td></tr>
<tr><td>114</td><td>NA</td><td>NA</td><td>Does the Bank is certified by ISO 27001 by an external party. Can you let us know the scope of this certification? Does it include all your processes, IT infrastructure, systems, Branches etc?</td><td>Yes.bank is certified with ISO 27001:2022 accreditions which cover the entire IT infrasructure</td></tr>
<tr><td>115</td><td>NA</td><td>NA</td><td>Is your Bank compliant with any of the following regulatory or compliance frameworks? (check all that apply and indicate most recent date of compliance)
<table>
<tr><th>Regulatory or Compliance Framework</th><th>Achieved Compliance</th><th>Most Recent Date of Compliance</th></tr>
<tr><td>ISO 27001:2013 Information security management systems</td><td>Yes/No</td><td></td></tr>
<tr><td>COBIT 5 (Control Objectives for Information and Related Technologies)</td><td></td><td></td></tr>
<tr><td>Payment Card Industry Data Security Standard (PCI DSS) (what level of requirement? 1/2/3/4)</td><td>Yes/No</td><td></td></tr>
<tr><td>HIPAA</td><td></td><td></td></tr>
<tr><td>General Data Protection Regulation (GDPR) of the European Union (EU)</td><td></td><td></td></tr>
</table></td><td>ISO 27001:2022 certification valid from 11-04-2023,
PCI DSS 3 valid from 01-08-2023</td></tr>
<tr><td>116</td><td>NA</td><td>NA</td><td>How is the inventory of current assets being manages specially from the point of interdependency and lifecycle of those assets?</td><td>We have automated inventory tool for tracking the assets and lifecycle.</td></tr>
<tr><td>117</td><td>NA</td><td>NA</td><td>Please let us know the details of following solution currently in use if not what compensatory solution used or in the absence of this function how this function is managed
a) Privileged Identity and Account Management ("PIM", "PAM")
b) Identity and Access Management ("IAM")
c) Security Information and Event Management (SIEM) and Let us know scope of SIEM Scope and confirm on, network security logs monitoring across all critical systems with 24*7 SOC monitoring (network traffic, Endpoint data, System log, System Event, User Analytics, cloud log)
d) Load Balancer in place to maintain the availability of critical resources
e) Next-Generation Web Application Firewall (WAF)
f) Next generation firewall (NGFW)
g) DDos attack prevention and detection
h) Intrusion detection systems (IDS) and intrusion prevention systems (IPS)</td><td>PIM, SIEM, IAM, Load balancer, WAF, NGFW, Anti DDos,IDS,IPS.

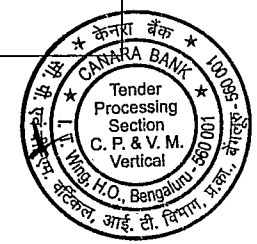
Details are confidential</td></tr>
</table>



Sl. No.	Section / Annexure / Appendix	RFP Clause	Bidders Query	Bank Response
118	NA	NA	Privileged Account Management a) How are privileged accounts secured and managed? i) Administrative users use different accounts for administrative use and non-administrative use (e.g. day to day activities) j) Standard users do not have administrative rights to their workstations k) Local administrator accounts are unique and complex on all systems l) A password management vault is used to manage privileged accounts m) MFA required for internal use of privileged accounts (e.g. when used for internal RDP connections) n) Other controls_____ b) Confirm on Whether Bank conduct detailed, Access control and User account review for all privileged user accounts and frequency of this review.	a)Privileged access is maintained through PIM i)Yes j)Yes k)Yes l)Yes m)Yes b)Yes
119	NA	NA	Data backups (i) Which systems are included in your backup strategy? [Business critical systems/All servers/All workstations/SaaS applications..etc] (ii) How frequently do you back up systems and data? [Continuously/Daily/Weekly/Monthly/Other frequency..etc] (iii) Are backups replicated and stored at multiple off-site locations? (iv) Are backups encrypted? (v) Along with online backups are offline backups maintained? (vi) Are processes in place for successful restoration and recovery of key assets within the RTO? (vii) Are backups periodically retrieved, compared to the original data to ensure backup integrity?	i)All databases ii) As per approved backup guidelines iii)Yes iv)Yes v)Yes vi)Yes vii)Yes
120	NA	NA	Is there encryption for ; (details in brief) Data at rest? Yes /No Data in transit? Yes / No Network (network level encryption)? Yes/No Endpoint devices (Laptops, tablets and removable media)? Yes/No	Data at rest? Yes Data in transit? Yes Network (network level encryption)? Yes Endpoint devices?Yes Details are confidential.
121	NA	NA	Please let us know how Bank gather threat intelligence as a proactive approach for your firm like intel feeds, dark web monitoring, IOC/IOA based approach etc	We have services for the same. And we receive Threat Intel Feeds from CSITE, Cert-In, NCIIPC, IB-Cart, & RSA Feeds
122	NA	NA	Information Security Policy: Does a Board approved information policy exist? Is this policy reviewed and updated annually or whenever there is a major change in the business environment?	Yes.
123	NA	NA	Information Security Policy: Is the Information Security Policy published and communicated to all the relevant internal and external stakeholders? Are other functional policie documented, approved by competent authority and communicated to all relevant stakeholders?	Yes,Information Security Policy is published and communicated to all the relevant internal and external stakeholders.Other Board approved functional policies are also in place and the same can be accessed by all the internal stakeholders.

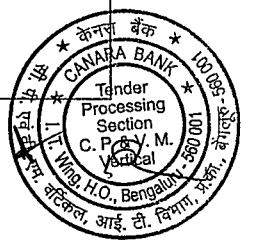


Sl. No.	Section / Annexure / Appendix	RFP Clause	Bidders Querry	Bank Response
124	NA	NA	Information Security Committee: Does the organization have established an Information Security Committee, with appropriate senior members from critical business functions? Is the information security organization chart is maintained? Are the responsibilities of the committee documented and communicated to all the committee members?	Yes,Information Secuirty Committee is established with appropriate senior members from critical business functions. Yes,Information secuirty Organisation chart is available. Responsibilities of committee are documented and communicated to all the commitee memebers.
125	NA	NA	Chief Information Security Officer: Is the Chief Information Security Officer or equivalent person appointed at adequately senior position? Does this information security position report to Chief Risk Officer or Chief Operating Officer or similar business function other than Information Technology?	Yes,Chief Information Security officer is heading Information Security Group of the Bank.Information Security Section comes under Risk Management Wing headed by CGM/Chief Risk Officer.
126	NA	NA	Segregation of Duties: Is the segregation of duties clearly defined and communicated for all the roles in information security?	Responsibilities of committee are documented and communicated to all the commitee memebers.
127	NA	NA	Contact with Authorities and Special Interest Groups : Does the organization have established and maintained contacts with authorities, such as, CERT-In, regulatory bodies, law enforcement agencies and special interest groups (e.g. ISACA)	Bank has established and maintained contacts with the Regulatory bodies
128	NA	NA	Information Security in Project Management: Does the organization have established Information security in project management regardless of the type of project?	Yes
129	NA	NA	Remote Working: Does organization allow remote working for its employees? Is the remote access to organization's information assets is adequately protected by applying suitable controls? Is 2FA implemented? Does the organization ensure only secured connections are utilized for remote users to ensure the confidentiality of sensitive information in transit?	Yes. Remote working is allowed after taking necessary permissions and ensuring security controls like MFA are in place. Remote Access Policy is also there.
130	NA	NA	Mobile Device Management: Does organization have implemented a Mobile Device Management (MDM) solution to secure its information on employee mobile devices, irrespective of the ownership (personal or Company provided)?	Yes
131	NA	NA	Background Verification Check: Does the organization conduct background verifiaction for all employees, contractors and third party staff to ensure knowledge and skills are in line with the job role, as well as, professional credentials of the prospective candidate?	Yes
132	NA	NA	Code of Conduct: Does organization have a documented "Code of Conduct", which includes information security related responsibilities of all employees, contractors and third party staff? Does the Code of Conduct is accepted and signed off by all the employees, contractors and third party staff? Does Code of Conduct sign off taken on annual basis or whenever there is a change ?	Yes



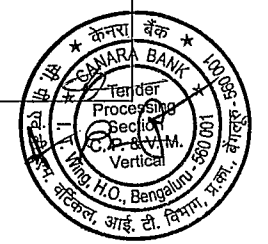
Sl. No.	Section / Annexure / Appendix	RFP Clause	Bidders Querry	Bank Response
133	NA	NA	Awareness Training : Does the organization conduct and measure general Information Security Awareness Training in every financial year to ensure all employees are aware of their responsibility towards information security and the cyber threats they might be susceptible to?	Our bank is regularly conducting training program on Cyber security for all our employees. Cyber Security is part of all our training programmes with duration of more than 3 days.
134	NA	NA	Phishing Simulation: Does the organization conduct simulated phishing campaigns every financial year, targeting business-sensitive employees within the organization and subsequently provide training for preparing employees to be more resilient and vigilant against phishing attacks?	Yes
135	NA	NA	Role Specific Security Training: Does the organization conduct domain-related security training tailored to specific roles for all employees (including senior management) in every financial year to ensure all employees are implementing effective cybersecurity concepts in their specific domain?	Program on Digital Awareness & Cyber Security is part of our Training Calendar, for employees from Scale I to III and SWOs . We are conducting seperate Certification programmes for Senior Management, CxO's & Board Members with IDRBT or other institutes recommended by RBI immediately after their induction.
136	NA	NA	Disciplinary Action: Does organization have a documented disciplinary action process for handling information security misbehaviour of the staff?	"Information Security violation/ Non-complaince of IT security guidelines/ guideline", is already covered in the Board Approved Staff Accountability Policy of the Bank
137	NA	NA	Post employment: Does the organization have documented "Post Employement" responsibilitites of the staff? Are they communicated to all the employees, contractors and third party staff?	Yes, for the employees of the Bank.
138	NA	NA	Asset Inventory: Does the organization maintain its hardware and network asset inventory to ensure that all assets are accounted for and protected adequately ?	Yes
139	NA	NA	Asset Inventory: Does the organization maintain an inventory of all its software licenses and subcscriptions to ensure optimum usage and license compliance?	Yes
140	NA	NA	Acceptable use : Does the organization have setup rules and controls towards acceptable use of its information assets? Are these rules communicated to all staff?	Yes,acceptable use of its information assets is defined in Information security policy and the same is communicated.
141	NA	NA	Information Classification: Does the organzation have a documented information classification scheme? How the information classification is done in practice?	Yes, as per the approved guidelines of the Bank.
142	NA	NA	Information Handling : Does the organization have a documented information handling procedure basis the information classification scheme?	Yes
143	NA	NA	Information Protection: How does the organization prevent unauthorised disclosure, modification, removal or destruction of information stored on media? How does the organization protect removable media, while in storage, in transit ?	Yes. Details are confidential.

Sl. No.	Section / Annexure / Appendix	RFP Clause	Bidders Querry	Bank Response
144	NA	NA	Data Disposal: Does the organization ensure effective disposal methods, like shredders, are used for properly disposing of confidential information in order to prevent attacks originating from information gathered by activities like dumpster diving?	Yes.
145	NA	NA	Data Disposal: Does the organization ensure effective disposal methods like degausser, to securely wipe off confidential information before disposing of the magnetic storage media e.g. hard disk drives?	Yes.
146	NA	NA	User Registration and De-registration: Does the organization have a formal documented user registration and de-registration process? Is the process automated or manual? Is the process aligned with HRs employee onboarding and off-boarding process?	Yes. Automated
147	NA	NA	User access provisioning: Does the organization have a formal documented user access provisioning process? Is the process automated or manual? Is the process aligned with HRs employee onboarding and off-boarding process? Is the access provided basis "need-to-know" basis and "least privilege" principle? Are users' access rights strictly controlled to only what they required to do their jobs?	User Access control / provisioning is defined and documented in IS Policy .
148	NA	NA	Privilege access control: How does the organization control privilege access rights allocation and use?	Management of Privileged Access Rights is defined in IS Policy.
149	NA	NA	Secrete access information: How does the organization allocate and communicate the secrete access credentials ? e.g. allocation of passwords, PINs, etc.	As per Bank's established Password policy
150	NA	NA	Protection of Secrete access information: Does organization make users responsible for protecting their secrete access information like login credentials (passwords, tokens, OTPs, etc.) ?	Yes,Password policy is in place
151	NA	NA	Password Policy: Has the organization implemented a password policy with a minimum password length of 8 or more characters, combination of lowercase and uppercase alphabets, numbers, and special characters, for all systems and applications to ensure adequate password complexity?	Yes,Password policy is in place
152	NA	NA	Changing Default Passwords: Does the organization ensure that the default passwords on all computer systems (e.g. routers) are changed to prevent entry in the organization network through a brute-force attack?	Endpoint default credentials are being centrally changed periodically for Windows endpoint desktops
153	NA	NA	Access Control Reviews: Does organization have a periodic access control review process implemented? How frequently access control reviews conducted and access reconcillication, re-certification is done?	Yes. As per the approved guidelines of the Bank
154	NA	NA	Adjustment or removal of access rights: Does the organization have a formal process established for adjustment of access rights basis internal transfers or role changes and removal of access rights when user leaves the organization?	Yes



Sl. No.	Section / Annexure / Appendix	RFP Clause	Bidders Querry	Bank Response
155	NA	NA	Restricted access to utility programs: Does organization restrict acces to utility programs that are capable of overriding system and application controls along with access to program source code?	Yes
156	NA	NA	User Accounts: Does the organization create dedicated user accounts with unique passwords for all personnel, including users with privileged access ?	Yes
157	NA	NA	User Accounts: Does the organization have a policy to automatically lockout user accounts not in use for certain number of days? E.g. more than 10 consecutive days?	Yes,defined in Password Policy
158	NA	NA	Privilege Identity and Access Management: Has the organization implemented a centralized privileged identity and access management (IAM) solution to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications?	Review of User Access Rights is defined in IS Policy.
159	NA	NA	Use of cryptographic controls: Does organization use cryptographic controls to protect its sensitive and critical information?	Yes
160	NA	NA	Management and protection of cryptographic information: How does the organization manages and protects its cryptographic keys, certificates, signatures, algorithms?	As per the defined Cryptography Policy which is included in IS Policy
161	NA	NA	Access to cryptographic information: How does the organization restricts access to its cryptographic keys, certificates, signatures, algorithms?	As per the defined Cryptography Policy which is included in IS Policy
162	NA	NA	Protecting against external and environmental threats: How does the organization protect itself from external and environmental threats like, malicious attacks, natural disasters, accidents?	-Strong defense in depth strategy and various cyber security controls -Strong BCP policy and periodic DR Drills -Physical security etc.
163	NA	NA	Physical Access Controls: Does the organization have implemented physical access control systems like proximity card or biometric access control?	Yes
164	NA	NA	Physical Access Controls: Does the organization have designated certain areas as restricted areas? (e.g. data center, server / network / electric / UPS rooms)	Yes
165	NA	NA	Physical Access Controls: Does the organization periodically reviews and updates access provided to restricted areas?	Yes
166	NA	NA	Environmental Controls: Does the organization have implemented adequate environment controls? such as, air conditioning, fire detection and suppression system, UPS, DG, water leakage detectors, etc.	Yes.In DC/DRC it is available.
167	NA	NA	Secure Disposal of Assets: Does the organization verify assets containing storage media to ensure that any sensitive information or licensed software has been removed or securely over-written prior to disposal or re-use?	Yes. Before disposal, all data will be removed securely through degaussing.

Sl. No.	Section / Annexure / Appendix	RFP Clause	Bidders Querry	Bank Response
168	NA	NA	Clear desk and clear screen : Does the orgnaization have documented Clear Desk and Clear Screen policy? Is the policy communicated to all users?	Yes.
169	NA	NA	Documented procedures: Does the organization have all the operational procedures documented?	Yes
170	NA	NA	Change Management: How does the organization controls changes to business processes, information processing facilities, systems and networks that affect information security?	Change management process is in place, periodic risk assesment is being conducted, proper testing and review are in place. Also, we are certified with ISO 27001:2022.
171	NA	NA	Capacity Management: Does the orgnanization monitor resource utilization, thresholds, and project the future capacity requirements to ensure optimum perfomance of its Information Systems?	Yes.
172	NA	NA	Segregation of environments: Does the organization have separated Development, Testing and Production environments to reduce the risk of unauthorised access or changes to the production environment?	Yes
173	NA	NA	Controls against malware: Does the organzation have implemented, malware detection, prevention and recovery technologies?	Yes
174	NA	NA	Patch Management: Does the organization timely, i.e. at least monthly, update IT systems and applications to prevent any known vulnerabilities being exploited?	Yes
175	NA	NA	System Hardening : Has the organization implemented security hardening of its end-user systems and servers to reduce the attack surface, giving attackers fewer opportunities to gain a foothold within your IT ecosystem?	Yes
176	NA	NA	Hardening of network devices: Has the organization implemented security hardening of its network devices, multifunction devices, printers, IP Telephony and video conferencing devices to reduce the attack surface, giving attackers fewer opportunities to gain a foothold within your IT ecosystem?	Yes
177	NA	NA	Information Backup and Restoration: Does the organization perform regular backups of business-critical data on servers to recover such data in cases of breaches, like ransomware attacks?	Data is being backed up on regular intervals as per approved backup guidelines.
178	NA	NA	Information Backup and Restoration: Does the organization ensure backups are regularly tested to validate the accuracy and integrity of the data and to verify the ability to restore data as quickly as possible with the least impact?	Backup and Restoration testing are being carried out on regular intervals as per approved guidelines.
179	NA	NA	Information Backup and Restoration: Does the organization perform regular backups of business-critical data on endpoints and ensure such backups are regularly tested to validate the accuracy and integrity of the data and their ability to restore data as quickly as possible with the least business impact in case of an attack like ransomware?	Not Applicable

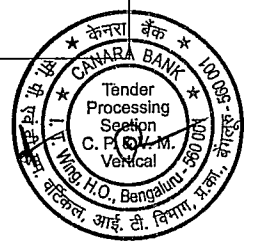


Sl. No.	Section / Annexure / Appendix	RFP Clause	Bidders Querry	Bank Response
180	NA	NA	Legacy Systems: Does the organization restrict the use of legacy (out of date/end of life) software and/or hardware that is officially not provided with security updates by manufacturers/providers (e.g. Windows XP) to prevent risk arising from legacy systems?	We are not using any legacy hardware /software related to servers.
181	NA	NA	Event Logging: Does the organization implement logging and monitoring of all systems or applications that process, transmit or store confidential information to identify any unauthorized security-related activities that may have been attempted or performed?	Yes
182	NA	NA	Protection of log information : Does the organization have controls implemented to protect the log information from tampering and unauthorized access?	Yes
183	NA	NA	Administrator and operator logs: Does the organization securely log administrator and operator activities and review them regularly?	Yes
184	NA	NA	Clock synchronization: Does the clocks of all relevant information processing systems synchronized to single reference time source?	Yes. Time is syncronized.
185	NA	NA	Installation of software on operational (PROD) systems: How does the organization controls installation of software on operational systems?	Not Applicable
186	NA	NA	Restrictions on software installations on end user systems: How does the organization controls installation of software on end user systems?	Application whitelisting policy and solution is in place to allow only authorised applications/utilities for endpoints
187	NA	NA	URL Filtering: Has the organization ensured that the standard security configuration of internal firewalls is individually adapted to prevent access to unauthorized external websites?	Yes
188	NA	NA	Application Filtering : Has the organization ensured that the standard security configuration of internal firewalls is individually adapted to prevent access to unauthorized applications?	Yes
189	NA	NA	Host Based Firewall: Has the organization implemented host-based firewall solutions on end-user devices and servers to actively identify and mitigate malicious traffic incoming to and outgoing from assets?	Yes
190	NA	NA	Advanced Persistent Threat (APT)/ Endpoint Detection and Response (EDR) : Has the organization implemented an Advanced Persistent Threat (APT) solution on end-user devices and servers to actively monitor and detect security threats based on system behavior?	Yes
191	NA	NA	Application Whitelisting : Has the organization implemented an application whitelisting solution on end-user devices and servers to limit the use of only authorized licensed applications on the assets?	Application whitelisting policy and solution is in place to allow only authorised applications/utilities for endpoints

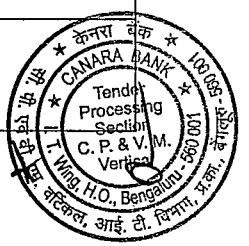
Sl. No.	Section / Annexure / Appendix	RFP Clause	Bidders Querry	Bank Response
192	NA	NA	Data Loss Prevention: Has the organization implemented a Data Loss Prevention (DLP) tool in monitor mode for making sure that end users do not send sensitive or critical information outside the corporate network?	Yes
193	NA	NA	Database Activity Monitoring : Has the organization implemented a Database Activity Monitoring (DAM) Solution to detect and prevent malicious behavior in the database?	Yes
194	NA	NA	Configuration Management Tool: Has the organization implemented a Configuration Management Solution (CMS) to conduct regular configuration security assessments on all organization-owned assets?	Yes
195	NA	NA	Patch Management Tool: Has the organization implemented a patch management solution to ensure that all critical and high-risk vulnerabilities reported are patched or mitigated within two days?	Yes
196	NA	NA	Anti-Malware: Has the organization implemented anti-malware or equivalent protection on end-user devices and servers that are updated/patched as per the vendor's recommendations to prevent malicious software attacks (e.g. IT virus, ransomware, spyware, etc.)?	Yes
197	NA	NA	Redundancy of IT infrastructure: What redundancies are leveraged in the design of your infrastructure ? (E.g, automatic failover logic, multiple processors, redundant I/O modules, Dual trunk networks)	Auto failover logic
198	NA	NA	Redundancy of IT infrastructure: Do you test updates and upgrades of firmware, software, web-applications and products of your systems before deployment?	Yes
199	NA	NA	Cloud Security Policy: Has the organization documented and implemented a cloud security policy to ensure security requirements are catered to when utilizing cloud services for business?	Cloud Security policy is available
200	NA	NA	Cloud Services Hardening: Has the organization taken measures to harden its cloud infrastructure as well as the services platform, inclusive of but not limited to identity and access management, encryption, and logging requirement to maintain the security hygiene of its cloud environment?	Yes
201	NA	NA	Technical vulnerability management: Does the organization conduct regular external penetration tests to identify vulnerabilities and exposure to associated risks? Does the organization identify and mitigate vulnerabilities and configuration flaws through security assessments conducted at least every financial year?	Yes
202	NA	NA	Segregation of networks: Does organization have segregated its network isolating into data center, DMZ, Management VLAN, and Guest VLAN to prevent the movement of an attacker in case of a breach?	Yes

Sl. No.	Section / Annexure / Appendix	RFP Clause	Bidders Querry	Bank Response
203	NA	NA	Information transfer security: Does organization have developed and established secure information transfer methodologies for transfer of business information between the organization and external parties?	Yes
204	NA	NA	Network & Security Devices Hardening: Has the organization implemented security hardening of its network and security devices to reduce the attack surface, giving attackers fewer opportunities to gain a foothold within your IT ecosystem?	Yes
205	NA	NA	Data Encryption: Does the organization implement encryption technology to protect sensitive and confidential information during transit and storage, as per the applicable compliance requirements and to prevent loss of confidential information in the event of a breach?	Yes
206	NA	NA	Wireless Security: Has the organization implemented strong authentication protocols for wireless networks to prevent attacks on wireless networks?	Not Applicable
207	NA	NA	Network Discovery: Has the organization implemented active and passive network discovery solutions capable of rogue device detection within their network so that only authorized devices are given access, while unauthorized and unmanaged devices are found and prevented from gaining access?	Yes
208	NA	NA	Network Access Control: Does the organization have a Network Access Control (NAC) solution in place to allow the organizations to restrict access to resources on their network and to prevent risk to the organization from Bring Your Own Device (BYOD), the internet of things (IoT), weak access permissions, and advanced persistent threats (APT)?	Yes
209	NA	NA	Deception Tools & Honeypots: Has the organization implemented a Deception Tools & Honeypots solution to divert and detect attackers with no risk to real data, operations, or users?	Yes
210	NA	NA	User Entity Behaviour Analysis: Has the organization implemented a User Entity Behavior Analysis (UEBA) solution on end-user devices and servers to detect anomalous behavior and to prevent insider threats/compromised users?	Yes
211	NA	NA	Intrusion Detection and Prevention: Has the organization implemented a Network-based Intrusion Detection and Prevention (NIDS/NIPS) solution to detect and prevent any malicious activity by monitoring the network traffic?	Yes
212	NA	NA	Firewall: 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

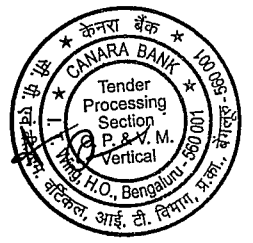
Sl. No.	Section / Annexure / Appendix	RFP Clause	Bidders Querry	Bank Response
213	NA	NA	Network Behaviour Anomaly Detection (NBAD): Has the organization implemented a Network Behaviour Anomaly Detection (NBAD) solution to continuously monitor the network for unusual events or trends that indicate a threat to the organization?	Yes
214	NA	NA	Web Application Firewall: Has the organization implemented a Web Application Firewall (WAF) capable of preventing the exploitation of web application vulnerabilities covering at least OWASP's Top 10 threats?	Yes
215	NA	NA	Host Intrusion Prevention System : Has the organization implemented a host-based intrusion detection and prevention solution (HIDS/HIPS) on end-user devices and servers to detect and prevent any malicious activity on assets?	Yes
216	NA	NA	Load Balancer: Has the organization implemented a Load Balancer to maintain the availability of critical resources?	Yes
217	NA	NA	DDOS Prevention: Has the organization implemented anti-Distributed Denial-of-Service (DDoS) solutions to prevent DDoS attacks?	Yes
218	NA	NA	Enterprise Threat Protection (ETP): Has the organization implemented an Enterprise Threat Protection (ETP) DNS proxy to detect and prevent any malicious activity ingress to the organization?	Yes
219	NA	NA	Browser Protection: Does the organization ensure the execution of only authorized and fully supported and updated web browsers that limit the execution of scripting language and that support only authorized plugins to minimize the attack surface and the opportunities for attacks that seek to manipulate human behavior through their interaction with web browsers?	Yes
220	NA	NA	Application Software Security: Does the organization ensure that it takes effective measures for managing the security life cycle of all in-house developed applications, like establishing secure coding practices appropriate to the programming language and development environment being used, only using up-to-date and trusted third-party components, and only using standardized, currently accepted, and extensively reviewed encryption algorithms, in order to prevent, detect, and correct security weaknesses?	Yes.
221	NA	NA	Application Software Security: Does the organization tests all the in-house developed software for functionality and security flaws, before implementing in the production environment, in order to prevent, detect, and correct security weaknesses?	Yes
222	NA	NA	Application Software Security: Does the organization include appropriate control clauses while buying commercial off the shelf (COTS) packaged software ?	Yes



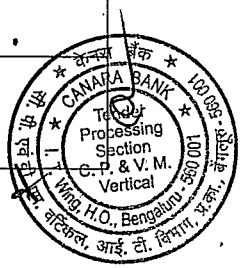
Sl. No.	Section / Annexure / Appendix	RFP Clause	Bidders Querry	Bank Response
223	NA	NA	Application Software Security: Does the orgnization takes adequate measures to ensure that source code and version control are maintained securely, for all in-house applications?	Yes
224	NA	NA	Application Software Security: Does the organization have escrow agreements for all critical applications sourced from third party (COTS)?	Yes
225	NA	NA	Application testing: Are in house developed applications tested prior to deployment into a production environment? Is there a rollback plan in the event a failure post implementation in production?	Yes
226	NA	NA	Application Hardening: Has the organization implemented measures to ensure the security hardening of applications, application servers, middleware, and databases to reduce the attack surface, giving attackers fewer opportunities to gain a foothold within IT ecosystem?	Yes
227	NA	NA	Database Security: Does organization have implemented security controls to protect critical databases? Such as DB hardening, DAM tool, etc.?	Yes, DAM Tool is in place
228	NA	NA	Securing Test Data : Does organization sanitize data being used for testing in UAT and preprod environments?	Yes
229	NA	NA	Contractual Agreements: Does organization include relevant information security clauses in critical supplier agreements?	Yes
230	NA	NA	Supplier Risk Assessments: Does the organization perform a cybersecurity risk assessment prior to conducting business with all suppliers and a continual assessment every financial year to ensure all security requirements are met?	Yes
231	NA	NA	Contractual Agreements: Does organization conduct periodic reviews of supplier security posture, at least annually once? And ensure that supplier implements recommended controls ?	Yes
232	NA	NA	Supplier Access Control: Does organization allow restricted access to suppliers basis least access principle? ("need to know" and "need to do")	Yes
233	NA	NA	Supplier Termination: Has the organization implemented the removal of system access, user accounts, and associated access rights as part of the process to terminate the contract with suppliers?	Yes
234	NA	NA	Incident Reporting, Investigation, and Recovery: Does the organization perform Incident Reporting, Investigation and Recovery effectively to ensure the recurrence rate of security events is minimal?	Yes



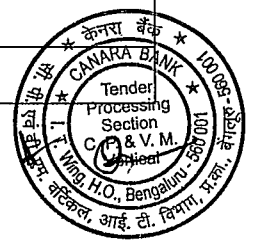
Sl. No.	Section / Annexure / Appendix	RFP Clause	Bidders Querry	Bank Response
235	NA	NA	SOC: Does the organization have a dedicated Security Operations Center (SOC) that is capable of monitoring, reporting, investigating and recovering any security incident observed within the organization's network?	Yes
236	NA	NA	Security Incident and Event Management Tool: Has the organization implemented a Security Incident and Event Management (SIEM) solution for proactively identifying, preventing, detecting, analyzing, and responding to security threats that the organization may face in a timely manner?	Yes
237	NA	NA	Cyber Crisis Management Plan: Has the Security Incident Response Plan been reviewed and approved by the organization's Board of Directors or persons with substantially similar responsibilities?	Yes
238	NA	NA	Cyber Crisis Management Plan: Does the Security Incident Response Plan include a review by the organization's legal counsel of laws or regulations that may affect the organization's response or other standards to which the organization may have to comply?	No
239	NA	NA	Cyber Crisis Management Plan Testing: Does the organization conduct a test for the IT Security Incident Response Plan and address the issues identified at least annually?	Yes.
240	NA	NA	DR Site: What is the type of DR site? Hot stand-by or warm stand-by?	Hot stand-by
241	NA	NA	DR Site: Is Disaster Recovery site is hosted in a different seismic zone?	Yes
242	NA	NA	DR Site : Does the organization have a Disaster Recovery (DR) site to allow it to continue business-sensitive operations in the event of a disaster?	Yes
243	NA	NA	DR Drill: Has the organization performed a Disaster Recovery (DR) drill to ensure the effectiveness and efficiency of its disaster recovery plan?	Yes
244	NA	NA	HA for Business Critical Assets: Does the organisation ensure a high availability of business critical infrastructure to ensure business continuity in case of an incident?	Yes
245	NA	NA	Red Team Exercises: Does the organization conduct regular red-teaming exercises to test organizational readiness for identifying/ responding quickly to vulnerabilities/attacks?	Yes



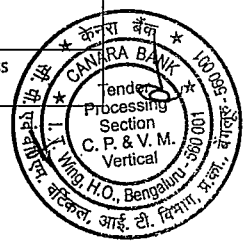
Sl. No.	Section / Annexure / Appendix	RFP Clause	Bidders Querry	Bank Response
246	NA	NA	Regulatory: Does the organization part of regulatory jurisprudence? Name the regulatory body. Does the organization ensure complince with the regulatory requirements? Has ever organization been found non-compliant in regulatory audits?	Yes. Name of regulators are RBI, SEBI, PFRDA,DFS, IRDAI, IFSCA,etc. Yes, we ensure the compliance with regulatory requirements. Regulatory audits is part of regulatory compliance .We enure that all the observations made during a regulatory audits are complied.
247	NA	NA	Statutory: Does the organization part of statutory jurisprudence? Name the statute that is applicable Does the organization ensure complince with the statutory requirements? Has ever organization been found non-compliant in statutory audits?	Yes, our bank is ensuring compliance to all the state, central goverments and other statutory laws applicable to us.
248	NA	NA	Legal: Does organization come under any international legal framework, like GDPR? Does the organization ensure complince with the applicable legal requirements? Has ever organization been found non-compliant in applicable legal audits? Has ever organization been penalized for breaching legal requirements?	Foreign branch of the bank in UK comes under GDPR.
249	NA	NA	Legal: Does organization comply with the IT Act of India, 2011 ?	Yes
250	NA	NA	Compliance: Have you implemented a procedure to permanently comply with all privacy relevant legislative statutory, regulatory and contractual requirements?	Yes.Data Protection policy is available.
251	NA	NA	Compliance: Do you have guidelines issued on the retention, storage, handling and disposal of records and information?	Yes
252	NA	NA	Compliance: Have you assigned a responsible person for providing guidance and ensuring awareness of privacy principles (e.g. Data Privacy Officer DPO)?	Yes
253	NA	NA	Compliance: What is the coverage of VAPT? When was the same last conducted? Was Log4shell and such, also included in the vapt scan conducted if not when would the same be conducted?	Periodic VAPT is being conducted covering all the asssets. Log4shell vulnerabilities are also scanned for.
254	NA	NA	Information security aspects of business continuity management: Have you conducted a Business Impact Analysis (BIA)? When was it last conducted?	Yes. It is being conducted annually
255	NA	NA	Information security aspects of business continuity management: Do you have a board approved Business Continuity Management (BCM) plan in place that specifically addresses cyber incidents?	Yes. For cyber incidents specifically, we have CCMP Plan.
256	NA	NA	Information security aspects of business continuity management: Do you test your information security continuity plans (e.g. Business Continuity Management, Disaster Recovery) at least annually?	Yes
257	NA	NA	Information security aspects of business continuity management: Are your information processing facilities (i.e. cyber systems, services or cyber infrastructure, or physical location housing it) implemented with redundancy?	Yes.



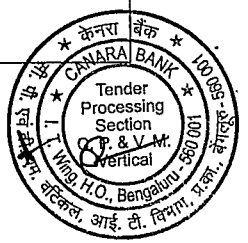
Sl. No.	Section / Annexure / Appendix	RFP Clause	Bidders Querry	Bank Response
258	NA	NA	Information security aspects of business continuity management: Please let us know how a typical BCP testing looks like in terms of Role played by different team and the process	BCP Review is conducted on regular intervals. Once approval is received from competent authorities, Tabletop Exercise will start by involving all the vendors, functional and technical groups. Then DR drill is conducted on approved date. Once all the applications involved starts working from standby , application team verifies all functions. Once verified, application works from standby side over a period of time. Post-Drill Actionable Measures is implemented to avoid reccurance. Also, drill Report is prepared and submitted to higher officials.
259	NA	NA	Information security aspects of business continuity management: Please explain in details. Please let us know how do you arrive at your RTO and RPO?	RTO and RPO is defined on BIA of individual applications based on its complexity, inter-dependency, functioning and criticality.
260	NA	NA	Information security aspects of business continuity management: What is the maximum acceptable outage or also known as RTO (Recovery Time Objective) for cyber systems? Please provide details on the same for critical and non critical systems.	RTO and RPO is defined on BIA of individual applications based on its complexity, inter-dependency, functioning and criticality.
261	NA	NA	Information security incident management: Do you have board approved information security incident response plan in place?	Yes
262	NA	NA	Information security incident management: Do all your employees and third party providers know the reporting line / escalation procedure for information security events / incidents?	Yes. The same is being communicated to all the stakeholders.
263	NA	NA	Information security incident management: Are employees and contractors required to report any identified information security weakness (not yet an incident or event) in systems or services?	Yes
264	NA	NA	Information security incident management: Do you use knowledge gained from analysing and resolving information security incidents to reduce the likelihood or impact of future information security incidents?	Yes
265	NA	NA	Information security incident management: Do you have segregation of network based on Business Function to avoid lateral spread?	Yes
266	NA	NA	Information security incident management: Are any data centers / networks / services being shared between the entities / subsidiaries to be covered / or even not covered under the policy please explain in detail?	No.Subsidiary entities network is not part of Bank's network
267	NA	NA	Supplier relationships: Have you identified and documented all your important suppliers / vendors (including third party service providers)?	Yes
268	NA	NA	Supplier relationships: Do agreements with third party service providers require levels of security commensurate with your own information security standard?	Yes
269	NA	NA	Supplier relationships: Do you monitor third party service provider / supplier activities for cyber security events to maintain an agreed level of information security?	Yes
270	NA	NA	System acquisition, development and maintenance: Does your web-server encrypt confidential data (e.g. HTTPS)?	Yes



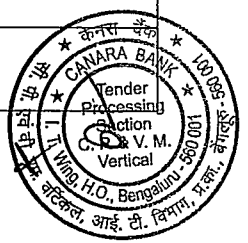
Sl. No.	Section / Annexure / Appendix	RFP Clause	Bidders Querry	Bank Response
271	NA	NA	System acquisition, development and maintenance: Do you test security functionality during the development lifecycle of information systems incl. IT security updates? If the response is no. request you to kindly share some more details on this aspect?	Yes
272	NA	NA	System acquisition, development and maintenance: Do you consider confidentiality when using operational data for testing to ensure that all sensitive details are protected by removal or modification?	Yes
273	NA	NA	Communications security: Are all internet access points secured by appropriately configured firewalls?	Not Applicable. We don't use Internet Access Points.
274	NA	NA	Communications security: Do you monitor your network and identify information security events?	Yes
275	NA	NA	Communications security: Are all internet-accessible systems (e.g. web-, email-servers) segregated from your trusted network (e.g. within a demilitarized zone (DMZ) or at a 3rd party provider)?	Yes
276	NA	NA	Communications security: Do you encrypt confidential communication (e.g. secure emails with SMIME (Secure Multipurpose Internet Mail Extensions) or SMTP-over-TLS (Simple Mail Transfer Protocol Secure))?	Yes
277	NA	NA	Communications security: Does the organization have network segregation implemented by isolating the demilitarized zone, InterVLAN communications, and Guest VLAN to prevent the movement of an attacker internally in case of a breach? Please explain intervlan security in detail?	Yes
278	NA	NA	Operations security: Have you implemented change management procedures for critical systems?	Yes
279	NA	NA	Operations security: Is the IT-environment for development and testing separated from production IT-environment?	Yes
280	NA	NA	Operations security: Do you use malware protection for all web-proxies, email-gateways, workstations and laptops?	Yes. However not applicable for web proxy.
281	NA	NA	Operations security: Besides traditional signature-based detection, does your malware protection use advanced heuristic- and behavioural-based detection mechanisms to protect against new malwares?	Yes
282	NA	NA	Operations security: Do you produce and regularly review event logs recording user activities, exceptions, faults and information security events (at least from your firewalls and domain controller) ?	Yes
283	NA	NA	Operations security: Have you implemented a centralized software installation process?	Yes
284	NA	NA	Operations security: Do you technically or organisationally ensure that employees must not install and, or run unauthorised portable softwares on their workstations? (Please share controls present excluding admin right restrictions being implemented)	Yes.Only whitelisted applications are allowed to install centrally.
285	NA	NA	Physical and environmental security: Do you maintain a list of personnel (employees, vendors and visitors) with authorized access to your premises and sensitive security areas?	Yes
286	NA	NA	Cryptography: Is all confidential information stored on mobile devices (e.g. smart phones, laptops) fully encrypted? If No, please elaborate.	Not Applicable. Mobile devices are not allowed to Access confidential information.



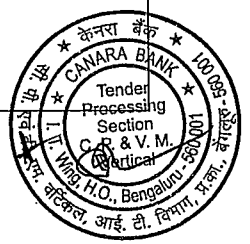
Sl. No.	Section / Annexure / Appendix	RFP Clause	Bidders Querry	Bank Response
287	NA	NA	Cryptography: Have you developed and implemented a policy on the use, protection and lifetime of cryptographic keys?	Yes
288	NA	NA	Access control: Do you restrict employees and external users privileges on a business-need to know basis (particularly administrative permissions, access to sensitive data e.g. personal data, etc.)?	Yes
289	NA	NA	Access control: Do you have a formal access provisioning process in place for assigning and revoking access rights?	Yes
290	NA	NA	Access control: Do you prohibit local admin rights on workstations for employees?	Yes
291	NA	NA	Access control: Do you review user access rights at least annually?	Yes
292	NA	NA	Access control: Do you revoke all system access, accounts and associated rights after termination of users (incl. employees, temporary employees, contractors, vendors, etc.)?	Yes
293	NA	NA	Access control: 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
294	NA	NA	Access control: Do you have PIM, PAM solution in place? If yes, please specify details including coverage of the solution being used?	Yes. PIM is in place for privileged access to servers.
295	NA	NA	Access control: Is multi factor authentication being used for all the cyber systems & services? If no what is coverage of the same in the organisation?	Yes
296	NA	NA	Access control: Are any of the manufacturing / logistic / generation systems / medical equipments. Either connected or dependant on IT systems which if not working might result in any loss?	Not applicable
297	NA	NA	Asset management: Do you keep an up-to-date inventory of software (incl. operating systems) and hardware assets being used in the organisation?	Yes
298	NA	NA	Asset management: Do you classify information, data with regards to confidentiality?	Yes
299	NA	NA	Asset management: Are information labelling procedures implemented in accordance with the above information classification scheme?	Yes
300	NA	NA	Asset management: Do you provide guidance on how to handle classified information?	Yes
301	NA	NA	Asset management: Do you either restrict access to, or encrypt confidential information stored on removable media like external storage devices (e.g. USB sticks or hard disks)?	Yes
302	NA	NA	Asset management: Do you securely dispose media containing sensitive information if it is not used any longer or if it needs to be disposed?	Yes



Sl. No.	Section / Annexure / Appendix	RFP Clause	Bidders Querry	Bank Response
303	NA	NA	Asset management: 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?	IT Assets and vendor management (ITAVM) solution is available for maintaining centralized inventory of hardware & software assets. It is a vendor solution.
304	NA	NA	Human resource security: Do you provide at least annual education to increase your users (employees and contractors) security awareness and prepare users to be more resilient and vigilant against phishing or cyber attacks?	Yes.
305	NA	NA	Human resource security: Do you have any User Behavioural Analytics tool (i.e. UEBA, etc.) to monitor patterns of human behaviour to detect anomalies from those patterns? Please explain in detail?	SIEM rules are in place to identify & detect anomalies in patterns of human behaviour
306	NA	NA	Organization of information security: Have you assigned a responsible person for information security (e.g. Chief Information Security Officer "CISO")?	Yes
307	NA	NA	Organization of information security: Do you have an up to date list of authorities and external contacts, which must be informed in case of an information security incident?	Yes
308	NA	NA	Organization of information security: Please list all the information security functions that exists (within the organization, via external vendor, MSP) to manage/perform day-to-day security tasks, functions (example: SOC, TI, IR, etc.)	Information Security functions include: 1. 24*7 monitoring in SOC 2. Incident response and management 3. Periodic internal VA and external VAPT 4. Red Team 5. DAST 6. Threat Hunting 8. Periodic Table Top Exercise & Drill 9. Periodic Phishing Simulation Exercise 10. Cyber Security Awareness 11. Action on Threat Intel Feeds received from CSITE, Cert-In, NCIIPC etc. 12. Regulatory Compliance
309	NA	NA	Organization of information security: Are any SaaS services being used, or provided? If yes who is responsible for the protection of data stored on the SaaS service? Please name the service provider being used?	Yes. Data stored is the responsibility of Service Provider. Multiple service providers are inducted.
310	NA	NA	Organization of information security: Please share future plans / roadmap for improving cyber security architecture including time frames to implement if any?	Data is confidential
311	NA	NA	Information security policies: Have you documented and implemented a board approved information security policy which is corporate-wide and permanently available for all employees and relevant external parties?	Yes
312	NA	NA	Information security policies: Has the organization documented and implemented a board approved cloud security policy to ensure cyber security requirements are catered to when utilizing cloud services for business?	Yes



Sl. No.	Section / Annexure / Appendix	RFP Clause	Bidders Querry	Bank Response
313	NA	NA	Technology implementation: Please share the update strategy followed in the organisation? 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? For all IT systems and applications to prevent any known vulnerabilities being exploited?	Yes
314	NA	NA	Technology implementation: Does the organization ensure that the default passwords on all computer systems (e.g. routers, etc) are changed to prevent entry in the organizations systems, networks through a brute force attack?	Yes
315	NA	NA	Technology implementation: Does the organisation ensure high availability of business critical cyber infrastructure to ensure business continuity in case of an cyber incident?	Yes
316	NA	NA	Technology implementation: 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 any disaster? How many data centers does the organisation have? When was the last DR drill conducted?	Yes. DR site is in place to continue operations in the event of any disaster. DR drills are conducted as per the approved BCP framework periodically.
317	NA	NA	Technology implementation: Does the organization have a dedicated or shared, Security Operations Center (SOC) either inhouse or outsourced that is capable of monitoring, reporting, investigating and recovering from any cyber security incident observed within the organization's cyber infrastructure?	Yes
318	NA	NA	Technology implementation: 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 internet of things (IoT), or weak access permissions, or advanced persistent threats (APT), etc?	Yes
319	NA	NA	Technology implementation: Has the organization implemented Deception Tool, or Honeypot solution to divert and detect attackers with no risk to real data, operations, or users?	Yes
320	NA	NA	Technology implementation: Has the organization implemented host-based firewall solution on end-user systems and servers to actively identify and mitigate malicious traffic incoming and outgoing from assets?	Yes
321	NA	NA	Technology implementation: Has the organization implemented an Endpoint threat Detection and Response (EDR) solution on all end point systems and servers to actively monitor and detect security threats based on system behaviour? Such as crowdstrike falcon EDR, etc.	Yes
322	NA	NA	Technology implementation: Has the organization implemented applications / softwares whitelisting solution on all end point systems and servers to restrict the use of only authorized applications / softwares on the assets? Please share controls present excluding admin right restrictions being implemented	Application whitelisting policy and solution is in place to allow only authorised applications/utilities for endpoints
323	NA	NA	Technology implementation: Has the organization implemented a Intrusion Detection and Prevention (IDS/IPS) solution for network, and host based on all end point systems to detect or prevent any malicious activity on IT assets by monitoring the network traffic?	Yes



Sl. No.	Section / Annexure / Appendix	RFP Clause	Bidders Querry	Bank Response
324	NA	NA	Technology implementation: Has the organization implemented a Data Leakage Prevention (DLP) tool on all end point systems and servers in blocking mode for making sure that end users do not send sensitive or critical information outside the corporate network?	Yes
325	NA	NA	Technology implementation: 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
326	NA	NA	Technology implementation: Does the organization ensure only secured connections like VPN are utilized by remote users to ensure the confidentiality of sensitive information in transit?	Yes
327	NA	NA	Technology implementation: 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? Please provide coverage of the solution being used? Does it cover IT and OT assets?	Security Incident and Event Management (SIEM) solution is in place for proactively identifying, preventing, detecting, analyzing, and responding to security threats and all servers and network devices are covered
328	NA	NA	Technology implementation: Has the organization implemented a Database Activity Monitoring (DAM) Solution to detect and prevent malicious behaviour in the database?	Yes
329	NA	NA	Technology implementation: Has the organization implemented anti-Distributed Denial-of-Service (DDoS) solution to prevent DDoS attacks?	Yes
330	NA	NA	Technology implementation: Please elaborate in details. What is the frequency of backup? How are backups taken? Please explain in detail the backup strategy & backup coverage being used in the organisation?	Data is being backed up on regular intervals as per approved backup guidelines.
331	NA	NA	Technology implementation: 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. virus, ransomware, spyware, etc.)? When were they last updated to the latest software version available?	Yes
332	NA	NA	Technology implementation: Please describe your current status with regards to Zero trust architecture for your network? What are the ongoing projects towards ZTA?	Bank has adopted Zero trust architecture. Further details are confidential.
333	NA	NA	Technology implementation: Do you have a process of real time monitoring for Domain admin accounts? Kindly elaborate?	Yes. Alerts are created and appropriate actions are being taken.
334	NA	NA	Technology implementation: Please describe your API security Framework?	Confidential, cannot be shared

Date: 05/02/2024
Place: Bangalore

Deputy General Manager

केनरा बैंक CANARA BANK Tender Processing Section C. P. & V. M. Vertical I. T. Wing, H.O., Bengaluru.-560 001