Area	Sr.No	Question	Bank RESPONSE
Demographics	**Basic Data**		
Demographics	1.1.1	Firm Name	Canara Bank
Demographics	1.1.2	Country	India
Demographics	1.1.3	Address	HEAD OFFICE 112, J C ROAD BENGALURU
Demographics	1.1.7	Primary Website(s)	www.canarabank.bank.in
Demographics	**Contact Information**		
Demographics	1.2.1	Primary Contact Name	Sivanantham V
Demographics	1.2.2	Primary Contact Title	Divisional Manager
Demographics	1.2.3	Primary Contact Role	Divisional Manager
Demographics	1.2.4	Primary Contact Email	sivananthamv@canarabank.com
Demographics	1.2.5	Primary Contact Phone	9597964957
Demographics	**ID Numbers**		
Demographics	1.3.1	Ticker Symbol	N.A
Demographics	1.3.2	DUNS Number	N.A
Demographics		**Basic Demographics**	
Demographics	1.4.1	Currency for all monetary responses.	INR Cr
Demographics	1.4.2	Revenue - Most Recent FY	83455.26 (as on Sep 30, 2025)
Demographics	1.4.3	Employee Count (approx.)	82000 (Approx.)
Demographics	1.4.4	Primary Industry (NAICS Code Look up	Banking
Demographics	1.4.5	Secondary Industry (NAICS Code Look up	N.A
Demographics	1.4.6	Tertiary Industry (NAICS Code Look up	N.A
Demographics	1.4.7	Please select geographies and indicate your organization's revenue allocation.	Available in Bank's Website
Demographics		Sum of Revenue	Available in Bank's Website
Demographics	1.4.8	Please select geographies and indicate your organization's employees allocation.	In India:81606 Outside:36
Demographics		Total Employees	82000 (Approx.)
Governance	**Security Organization**		
Governance	2.1.1	Please provide an overview of the organization's information/cybersecurity structure:	Bank has a dedicated Cyber Security Wing that manages information and cyber security, incident response, security operations,security assessments which is headed by CISO. CISO office directly reprots to Executive Director overseeing Cyber security function. We have an Information Security Committee in place which is chaired by Executive Director.All the technical wing/vertical heads are members of IS committee. NCIIPC Director (South), is a permanent Invitee to the ISC. Further all the Cyber security related aspects are being discussed extensively in IT-Strategy Committee & Board. Wing is having a Cyber-Security operations centre which monitors all the IT infrastructure 24*7*365.

Area	Sr.No	Question	Bank RESPONSE
Governance	2.1.2	Overall Information Technology Budget (most recent FY)	Confidential information
Governance	2.1.3	Percentage of your IT budget allocated to information/cybersecurity (approx.).	Confidential information
Governance	2.1.4	Overall Information/Cybersecurity Budget (most recent FY)	**Confidential information**
Governance	2.1.5	Our information/cybersecurity organization is:	
Governance		Centralized (e.g. There is a centralized information/cybersecurity function which oversees all business units)	Yes
Governance		Decentralized (e.g. Business units are individually responsible for information/cybersecurity functions)	NA
Governance		Federated/Hybrid (e.g. Business units have day-to-day management control, but there are centralized information/cybersecurity policies and standards)	NA
Governance	**Security Officers**		
Governance	2.2.1	The organization has a Chief Information Security Officer (CISO), Chief Security Officer (CSO) or functional equivalent. (If yes, please provide name in additional commentary)	Yes, Details available in public domain.
Governance	2.2.2	If you answered Yes to statement 2.2.1, please indicate to whom the individual reports.	The CISO reports directly to the Executive Director overseeing the Cyber Security function.
Governance	2.2.3	If you answered Yes to statement 2.2.1, does that individual periodically, but not less than annually, brief the board of directors or an equivalent if a non-public organization?	Yes, CISO reports periodically to the board about the organisations cyber security preparedness as per RBI Cyber Security Framework
Governance	2.2.4	The organization manages cyber/information security risks by: *(check all that apply)* .	
Governance		Performing a cybersecurity risk assessment at least annually to identify risks, analyze risks, assess likelihood, assess impact, prioritize risks, plan response strategies, and monitor, evaluate, and adjust.	Yes
Governance		Documenting the results of the annual cybersecurity risk assessment/management in a report that includes prioritized risk response actions including accept, transfer, mitigate, or avoid.	Yes
Governance		Presenting the Cybersecurity Risk Assessment Report to the Board, or equivalent at least annually.	Yes
Governance	2.2.5	The organization has a Chief Privacy Officer (CPO) or a functional equivalent. (if yes, please provide name in additional commentary)	Yes

Area	Sr.No	Question	Bank RESPONSE
Governance	**Security Policies and Standards**		
Governance	2.3.1	The organization documents and implements enterprise or company-wide policies/programs (select all that apply):	
Governance		Cyber / Information Security Policy.	Yes
Governance		Acceptable Use Policy (AUP) that defines for all parties the ranges of permitted use of organizationally-provided technologies; contains consequences for noncompliance/violation of the AUP.	Yes
Governance		Users are disallowed from surfing social media platforms from organizational assets except where this is a defined business need.	Yes
Governance		Insider Threat Program coordinated capabilities to deter, detect, and mitigate insider threats.	Yes
Governance	2.3.2	The following cybersecurity standards, frameworks, or best practices are leveraged by the organization:	
Governance		ISO/IEC 27001 'Information Security Management System (ISMS)'	Yes
Governance		NIST Special Publications aimed at computer/cyber/information security	Yes
Governance		Center for Internet Security 'Critical Security Controls'	Yes
Governance		ISACA 'COBIT'	Yes
Governance		FFIEC 'Cybersecurity Assessment Tools'	Not Applicable
Governance		NIST Cybersecurity Framework (NIST CSF)	Yes
Governance		PCI-DSS	Yes
Governance		HIPAA Security	Not Applicable
Governance		Information Security Forum (ISF), Standard of Good Practice for Information Security	No
Governance		Others **(please describe):**	Bank is complying with the Alerts,Advisories and best practices issued time to time from CERT-In, NCIIPC, SEBI,DSIC, RBI etc.
Governance	2.3.3	The organization has documented enterprise or company-wide Privacy Policies (please note policy titles, the version, and date released)	Yes (Website Privacy Policy/Notice and DPDP policy as Draft)
Governance	2.3.4	The organization implements a physical security program with risk-based protections (e.g., CCTV, visitor access controls, badge access, and alarms for the perimeter) to secure offices and data center facilities.	Yes
Governance	2.3.5	Our screening and background check requires background verification checks including criminal records, credit history, education and reference checks, and employment history as permitted by law. *(please check all that apply)* .	
Governance		Employees	Yes
Governance		Contractors/ Consultants	Yes
Governance	**Independent Audit / Assessment**		

Area	Sr.No	Question	Bank RESPONSE
Governance	2.4.1	The organization engages with an independent service provider to: a) conduct an assessment of our information/cybersecurity program and associated controls. b) prepare and deliver a report that documents the results of the assessment and recommendations for improvement.	a)Yes b)Yes
Governance	2.4.2	Our internal Audit department conducts risk-based audits or assessments of the information/cybersecurity program and associated controls on an annual or more frequent basis.	Yes
Data Protection		**Records**	
Data Protection	3.1.1	Number of **records in the custody** of the organization by PCI (Payment Card Industry/Information).	(Credit card+ Debit Card base)= Approx 6.20 Cr+
Data Protection	3.1.2	The PCI Information provided above is an estimation?	Yes
Data Protection	3.1.3	Number of **records in the custody** of the organization by PHI (Protected Health Information) / Sensitive Personal Data.	Not Applicable
Data Protection	3.1.4	The PHI Information provided above is an estimation?	Not Applicable
Data Protection	3.1.5	Number of **records in the custody** of the organization by PII (Personally Identifiable Information) / Personal Data.	Approx 12 Cr
Data Protection	3.1.6	The PII Information provided above is an estimation?	Yes
Data Protection	3.1.7	The organization processes and/or transacts records on behalf of others, e.g. a payment processor.	Yes
Data Protection	3.1.8	Number of **records processed and/or transacted** by the organization annually by PCI (Payment Card Industry/Information).	6.2+ Cr
Data Protection	3.1.9	The PCI Information provided above is an estimation?	Yes
Data Protection	3.1.10	Number of **records processed and/or transacted** by the organization annually by PHI (Protected Health Information) / Sensitive Personal Data.	Not Applicable
Data Protection	3.1.11	The PHI Information provided above is an estimation?	Not Applicable
Data Protection	3.1.12	Number of **records processed and/or transacted** by the organization annually by PII (Personally Identifiable Information) / Personal Data.	Approx 12 Cr
Data Protection	3.1.13	The PII Information provided above is an estimation?	Yes
Data Protection	**Information Control**		
Data Protection	3.2.1	The organization regularly handles or processes information owned by other organizations, unrelated companies, or external customers *(please check all that apply)*.	
Data Protection		Personally Identifiable Information (PII)	Yes
Data Protection		Protected Health Information (PHI)	No
Data Protection		Intellectual Property/Trade Secrets/Marked Confidential Information	Yes
Data Protection		Sales/Business Projections	Yes
Data Protection		Merger & Acquisition/Business Development	Yes
Data Protection		Insider Financial Information (e.g., non-public information related to a publically traded company's earnings, forecasts, and acquisition and divestiture plans)	Yes
Data Protection		Product Development / Research & Development	Yes
Data Protection		Advertising / Marketing / Product Roadmaps	No
Data Protection		Government Classified Data	Yes, If required.
Data Protection		Other (please describe below):	

Area	Sr.No	Question	Bank RESPONSE
Data Protection	3.2.2	We encrypt account usernames and authentication credentials during transmission over an IT network (i.e., we do not permit clear text usernames and authentication credentials across networks).	Yes
Data Protection	3.2.3	The organization utilizes mandatory encryption to protect critical information and other sensitive information (e.g., PII, PHI, etc.) as defined by information classification and protection policies.	
Data Protection		Data at Rest	Yes
Data Protection		Data in Transit	Yes
Data Protection		Corporate laptops and desktops	Yes
Data Protection		Data on Removable media	Yes
Data Protection		Mobile Devices (e.g., Mobile phones and tablets)	Yes
Data Protection		Backups	Yes
Data Protection	**Media Disposal**		
Data Protection	3.3.1	Our organization maintains data disposal/ sanitization policies that define media (e.g., hard drives, CDs, USB storage devices, etc.) sanitization requirements and techniques.	Yes
Data Protection	3.3.2	We have procedures or contracts with service providers to sanitize items or media with sensitive/confidential information prior to reuse or to disposal.	Yes
Inventory and Control of Enterprise Assets	**Inventory all hardware devices**		
Inventory and Control of Enterprise Assets	4.1.1	The percentage of hardware connected to the organization's network is inventoried is	100%
Inventory and Control of Enterprise Assets	4.1.2	The organization's hardware asset inventory is updated at least:	Continuously
Inventory and Control of Enterprise Assets	**Track all hardware devices**		
Inventory and Control of Enterprise Assets	4.2.1	The organization's hardware inventory is documented:	Yes.Bank maintains centralized IT Asset Inventory.
Inventory and Control of Enterprise Assets	4.2.2	An automated asset inventory and discovery tool provides visibility to the following percentage of hardware across the enterprise?	Yes
Inventory and Control of Enterprise Assets	4.2.3	We leverage our automated asset inventory tool's discovery capabilities to help detect unknown or unauthorized devices, and to improve the accuracy of our inventory.	Yes
Inventory and Control of Enterprise Assets	4.2.4	Our active discovery tool is configured to execute at least:	Daily. Endpoints are being scanned centrally during business hours on a daily basis.
Inventory and Control of Enterprise Assets	**End of Life (EOL) Technology**		
Inventory and Control of Enterprise Assets	4.3.1	Our organization relies on operating systems, software, or hardware that is no longer supported or is considered "end-of-life" (EOL) by the manufacturers. (If yes, summarize EOL cases)	No
Inventory and Control of Enterprise Assets	4.3.2	End-of-life technologies in use by the organization: (select all that apply)	
Inventory and Control of Enterprise Assets		Are segregated from the rest of the network	Yes
Inventory and Control of Enterprise Assets		Have additionally purchased extended support for the software, where available.	Yes

Area	Sr.No	Question	Bank RESPONSE
Inventory and Control of Enterprise Assets		Other (please add comments describing compensating controls, or summarize milestone dates or target dates to upgrade to a supported platform)	The bank ensure that no devices remain beyond End-of-support status, and appropriate support measures are implemented for any EOL system.
Inventory and Control of Software Assets	**Inventory all Software**		
Inventory and Control of Software Assets	5.1.1	We maintain an inventory of software in use across the organization.	Yes
Inventory and Control of Software Assets	5.1.2	If yes to statement 5.1.1, the inventory captures what percentage of software, including version, that is in use throughout the enterprise.	100%
Inventory and Control of Software Assets	5.1.3	Our inventory of software installed on enterprise assets is updated at least:	As and when renewal is due
Inventory and Control of Software Assets	**Software and Hardware Inventory Tools**		
Inventory and Control of Software Assets	5.2.1	The organization's software inventory is documented:	Yes
Inventory and Control of Software Assets	5.2.2	An automated software inventory tool provides visibility to the following percentage of information systems across the enterprise:	Yes
Inventory and Control of Software Assets	5.2.3	Our inventory of software is:	
Inventory and Control of Software Assets		All supported.	
Inventory and Control of Software Assets		**All supported, other than those with documented exception with mitigating controls.**	Yes
Inventory and Control of Software Assets		**Updated with a process repeated at least monthly.**	
Inventory and Control of Software Assets	**File Integrity Tools (Allowlisting)**		
Inventory and Control of Software Assets	5.3.1	In concert with the software inventory, our file integrity checking tools validate software has not been modified prior to execution on a system.	Yes
Inventory and Control of Software Assets	5.3.2	**Our application allowlisting technology is configured to allow critical systems to run software only if it is included on our allowlist. (Describe the allowlisting solution and indicate the name of the solution provider below).**	Yes
Secure Configuration of Enterprise Assets and Software	**Security Configuration Management**		
Secure Configuration of Enterprise Assets and Software	6.1.1	We implement standard secure configuration images for operating systems and software applications.	Yes for Operating Systems. Not available for software applications
Secure Configuration of Enterprise Assets and Software	6.1.2	We implement secure configurations (incorporating industry recognized security hardening techniques, e.g., Center for Internet Security (CIS) Security Configuration Benchmarks or NIST security configuration checklists, etc.) for the following percentage of our operating systems and software applications:	Yes
Secure Configuration of Enterprise Assets and Software	6.1.3	Our system configuration management tools (e.g., Active Directory Group Policy, etc.) enforce and redeploy configuration settings to systems.	Yes
Secure Configuration of Enterprise Assets and Software	**Information System Change Tools**		
Secure Configuration of Enterprise Assets and Software	6.2.1	In our organization, the development, testing, and production IT environments are separated.	Yes

Area	Sr.No	Question	Bank RESPONSE
Secure Configuration of Enterprise Assets and Software	6.2.2	Our formal system/application change control policy requires risk assessment, security testing, authorization, and establishment of roll-back procedures prior to deployment into our production environment.	Yes
Secure Configuration of Enterprise Assets and Software	**User Activity Lockout**		
Secure Configuration of Enterprise Assets and Software	6.3.1	In our organization, user accounts are automatically logged off after a standard period of inactivity.	Yes
Secure Configuration of Enterprise Assets and Software	6.3.2	In our organization, accounts are locked out after a set number of failed login attempts and accounts either automatically unlock after a standard period of time or end-users contact the helpdesk to unlock accounts.	Yes
Audit Log Management	**Audit Logs and Records**		
Audit Log Management	7.1.1	We implement standard audit logging policies for hardware devices and software.	Yes
Audit Log Management	7.1.2	Whenever possible, our system logs are kept in a standardized format, such as syslog entries or the Common Event Expression.	Yes
Audit Log Management	7.1.3	We maintain audit logs for a period of no less than (select from list):	The time period varies for different types of audit logs, with not less than 6 months.
Audit Log Management	7.1.4	The organization enforces detailed audit logging of access or changes to sensitive data.	Yes
Audit Log Management	**Audit Log Collection**		
Audit Log Management	7.2.1	We configure our network boundary devices including: firewalls, network-based Intrusion Prevention System (IPS), and inbound and outbound proxies to log traffic based on your cybersecurity policies.	Yes
Audit Log Management	7.2.2	Our organization uses Active Directory:	Yes
Audit Log Management	7.2.3	Select all of the Audit Policies enabled on Domain Controllers:	
Audit Log Management		Audit Credential Validation (Failure)	Yes
Audit Log Management		Audit Process Creation (Success)	Yes
Audit Log Management		Audit Security Group Management (Success and Failure)	Yes
Audit Log Management		Audit User Account Management (Success and Failure)	Yes
Audit Log Management		Audit Other Account Management Events (Success and Failure)	Yes
Audit Log Management		Audit Sensitive Privilege Use (Success and Failure)	Yes
Audit Log Management		Audit Logon (Success and Failure)	Yes
Audit Log Management		Audit Special Logon (Success)	Yes
Audit Log Management	**Audit Anomaly Reviews**		
Audit Log Management	7.3.1	Our organization analyzes audit logs/reports/alerts on a regular basis to identify anomalies or unusual activities.	Daily
Audit Log Management	7.3.2	Our security personnel and/or system administrators actively review anomalies to identify unauthorized activities and resolve incidents via our incident response and management processes.	Yes

Area	Sr.No	Question	Bank RESPONSE
Network Monitoring and Defense	**Security Operations Center / SIEM**		
Network Monitoring and Defense	8.1.1	The organization operates its own Security Operations Center (SOC) and/or has an outsourced Managed Security Service Provider (MSSP) with the following capabilities at a minimum: a) Established incident alert thresholds b) Security Incident and Event Management (SIEM) monitoring and alerting for unauthorized access connections, devices, and software.	Our Bank operates it's own Security Operations Centre(SOC) with established incident alert thresholds and SIEM based monitoring and alerting for any unauthorised access, connection, devices, and software.
Network Monitoring and Defense	8.1.2	The SOC/MSSP capabilities include, but are not limited to, the following: a) 24x7 operations b) mix of signature and heuristic-based detection c) incident response, containment, and remediation capabilities d) active threat intelligence and analytics delivering rapid alerts/notification and/or countermeasures e) processes are continuously improved.	SOC operates 1.24*7*365 2.Mix of signature and heuristic based- use cases are available in SIEM 3.Board approved Cyber Crisis Management plan is in place with incident response, containment, and remediation capabilities. 4.For threat intel, we have onboarded M/s.IZoologic & M/s CloudSek. we are also receiving feeds from M/s.IBCART, NCIIPC& various regulatory authorities. 5. All the use cases/processes are being reviewed periodically and are being improved continuously.
Network Monitoring and Defense	8.1.3	We implement a SIEM (Security Information and Event Management) or log analytic tool for unified aggregation, consolidation, correlation, analysis, and alerting.	Yes
Network Monitoring and Defense	8.1.4	We continuously refine and tune our SIEM (e.g., profiling common system events to tune detection towards unusual activity) to minimize false positives and insignificant alerts.	Yes
Network Monitoring and Defense	8.1.5	Our Security Operations Center / Managed Security Service Provider (SOC/MSSP) obtains relevant indicators of compromise (IOCs) combined with leveraging threat intelligence feeds to rapidly discover and respond to threats. (e.g., correlate IOC and identify and alert on threat actors targeting the organization).	Yes
Network Monitoring and Defense	8.1.6	Our security operations center or third party provider monitors the US-CERT, industry-related Information Sharing and Analysis Center (ISAC), and other feeds for alert and threat information; this information is reviewed and actions taken to mitigate risks.	Yes,IB-Cart/CERT-In feeds are added in & relevant use cases are created in SIEM tool for monitoring.
Network Monitoring and Defense	**Intrusion Detection and Prevention Systems**		
Network Monitoring and Defense	8.2.1	Our organization deploys intrusion detection and prevention security devices at network egress points to detect and prevent attacks through the use of signatures, network behavior analysis, and other mechanisms.	Yes
Network Monitoring and Defense	8.2.2	Our intrusion prevention systems (IPS) are deployed in an active block mode - to block known bad signatures, malicious activities/ code, and sophisticated attack behaviors.	Yes
Network Monitoring and Defense	8.2.3	Our organization routes all outbound web requests through a web proxy which monitors for and blocks potentially malicious content.	Yes
Account Management	**Identity and Access Management**		
Account Management	9.1.1	Please describe the organization's remote access protocols (e.g., Remote Desktop Protocol RDP, VPN, Telnet, etc.) to the corporate network and how the organization secures remote access for each protocol.	Accops Work from Home solution provides remote access to limited number of authorised users through a secured VPN channel with the underlying protocol being RDP. Additional controls such as AD integration for authentication, MFA, device compliance checks etc. are in place for
Account Management	9.1.2	Select all responses that are true: Which of the following tools does the Applicant use for directory services, identity providers (IdP), federation and/or rights management?	
Account Management		Microsoft Active Directory (Active Directory)	Yes
Account Management		Azure Active Directory (Azure AD)	No
Account Management		Okta	No
Account Management		Ping	No
Account Management		Active Directory Federation Services	Yes

Area	Sr.No	Question	Bank RESPONSE
Account Management		Google Workspaces	No
Account Management		Other (details required – provide in the comments below)	
Account Management		None of the above/Don't Know.	
Account Management	9.1.3	Select one response: What is the source of identity for the majority of Applicant's users?	Active Directory
Account Management	9.1.4	Select all responses that are true: With regards to how the Applicant protects "Privileged" "Service Accounts":	
Account Management		There is an inventory of all "Privileged" "Service Accounts", and it is updated at least quarterly.	Yes
Account Management		"Privileged" "Service Accounts" have password lengths of at least 25 characters.	No
Account Management		"Privileged" "Service Accounts" have their passwords rotated at least annually.	Yes
Account Management		"Privileged" "Service Accounts" have their passwords rotated at least quarterly.	No
Account Management		"Privileged" "Service Accounts" are configured using the principle of least privilege.	Yes
Account Management		"Privileged" "Service Accounts" are configured to deny interactive logins.	Yes
Account Management		Specific monitoring rules are in place for Privileged Service Accounts to alert your Security Operations Center (SOC) of any abnormal behavior.	Yes
Account Management		Service Accounts are tiered such that different accounts are used to interact with workstations, servers, and authentication servers, even for the same service.	Yes
Account Management		There is a process in place to review at least annually the current requirements for each service associated with "Privileged" "Service Accounts" to verify the service still requires the permissions the service account has (and deprivilege if not).	Yes
Account Management		None of the above/Don't know.	
Account Management	9.1.5	Indicate the number of active accounts the organization has for Domain Administrator Accounts. Accounts should not include inactive accounts, but should include all nested accounts aggregated across all domains/forests.	11
Account Management	9.1.6	Indicate the number of active accounts the organization has for Privileged Services Accounts. Accounts should not include inactive accounts, but should include all nested accounts aggregated across all domains/forests.	4
Account Management	9.1.7	Indicate the number of users who have persistent administrative access to servers and/or workstations other than their own.	0
Account Management	9.1.8	The organization's posture with respect to access controls for member servers is best described as: Note: *This question is regarding employees' everyday user accounts; where the Applicant provisions employees with separate credentials for administrative access, those accounts should not be considered for the purposes of this question*	Some of the Applicant's employees are in the Administrators' group or are local admins. Admin access and everyday user accounts are separate.
Account Management	9.1.9	Select all responses that are true: With regards to how the Applicant protects user accounts with domain administrative privileges ("Domain Administrator Accounts"):	
Account Management		System administrators have a unique, privileged credential for administrative tasks (separate from their user credentials for everyday access, email, etc.).	Yes
Account Management		Domain Administrator Accounts require multifactor authentication.	Yes
Account Management		Domain Administrator Accounts are managed and monitored through just-in-time access, are time bound, and require approvals to provide privileged access.	Yes
Account Management		Domain Administrator Accounts are kept in a password safe that requires the user to "check out" the credential (which is rotated afterwards).	No

Area	Sr.No	Question	Bank RESPONSE
Account Management		In addition to being kept in a password safe, Domain Administrator Accounts are not exposed to the administrative user when "checked out", and access is recorded through a session manager.	No
Account Management		Domain Administrator Accounts can only be used from Privileged Access Workstations (workstations that do not have access to internet or email).	Yes
Account Management		There is a log of all actions by "Domain Administrator Accounts" for at least the last thirty days.	Yes
Account Management		None of the above/Don't Know.	
Account Management	**Account Management and Review**		
Account Management	9.2.1	We review user accounts at least annually to confirm all accounts are associated with a valid end-user.	Yes
Account Management	9.2.2	We review service/system accounts at least annually and disable any account that cannot be associated with a valid business process and owner.	Yes
Account Management	9.2.3	We review user, administrative, and privileged accounts at least (select from list) to confirm all accounts are associated with a valid user.	Annually
Account Management	9.2.4	We monitor user accounts and flag dormant accounts (e.g., accounts with no activity for over 60 calendar days) and consult with the corresponding manager prior to disabling the account.	Yes
Account Management	**Password Policies**		
Account Management	9.3.1	Our organization's technical controls enforce the following password requirements (select all that apply):	
Account Management		Minimum number of characters	Yes
Account Management		Complexity (e.g., lowercase, uppercase, numbers, or symbols) requirements	Yes
Account Management		Prohibit reuse	Yes
Account Management		Blocking known weak passwords (e.g., "1q2w3e4r5t" and "Passw0rd!")	Yes
Account Management		Detects known compromised/breached passwords from dark web and other sources, and enforces a password reset	Yes
Account Management		Passwords expiration (change is required) at least annually	Yes
Account Management	9.3.2	If there are technological limitations preventing multi-factor authentication, then we enforce complex long passwords (i.e., longer than 14 characters).	Yes
Access Control Management	**Account Monitoring and Revocation**		
Access Control Management	10.1.1	In our organization, user accounts have an expiration date which is monitored and enforced.	Yes
Access Control Management	10.1.2	We follow a process to disable user accounts upon termination of an employee, contractor/consultant, or third party user.	Yes
Access Control Management	10.1.3	We follow a process to disable system accounts upon termination of an employee, contractor/consultant, or third party user.	Yes
Access Control Management	**Privileged Access Management**		
Access Control Management	10.2.1	We limit the use and distribution of administrator or privileged accounts (select all that apply):	
Access Control Management		Via an account authorization process requiring senior management approval.	No
Access Control Management		Administrative/Privileged credentials are separate from credentials used to perform day-to-day tasks.	Yes
Access Control Management		Administrators are explicitly disallowed from surfing the internet or accessing personal email from their privileged accounts.	Yes
Access Control Management	10.2.2	The organization manages Desktop / Local Administrator privileges via: Please check all that apply and indicate the name of the solution(s) below:	
Access Control Management		Endpoint Privilege Management (EPM)	
Access Control Management		Local Administrator Password Solution (LAPS) or an equivalent solution that sets a different, random password for the common local administrator account across all domain-attached computers.	Yes

Area	Sr.No	Question	Bank RESPONSE
Access Control Management		Privileged Access or Account Management (PAM)	
Access Control Management		Other (please describe below):	
Access Control Management	10.2.3	The organization implements a Privileged Account Management (PAM) solution that, (select all that apply, and add a comment with the name of your PAM solution)	
Access Control Management		Controls access to administrative/privileged accounts	Yes
Access Control Management		Monitor, record, audit and analyze administrative/privileged access, sessions, and actions	Yes
Access Control Management		Automated credential management (i.e., credentials automatically rotate after each use or the use of temporary one-time use passwords)	Yes
Access Control Management	10.2.4	The scope of our PAM implementation includes, (check all that apply):	
Access Control Management		Application Accounts	
Access Control Management		Break glass (emergency or firecall) accounts	
Access Control Management		Domain administrative accounts	Domain Administrative Accounts are available in Active Directory which are use for administration of the domain. These accounts are separate from the accounts used for day-to-day operations and the access to Active Directory using these accounts happens only over PIM solution
Access Control Management		Service accounts	
Access Control Management		Windows local accounts	
Access Control Management		Windows server local accounts	Yes
Access Control Management	**Multi-Factor Authentication**		
Access Control Management	10.3.1	Our organization uses the following secondary factor methods for MFA:	
Access Control Management		SMS	Yes
Access Control Management		Biometric authentication	Yes
Access Control Management		Authenticator application	Yes
Access Control Management		Secondary email	
Access Control Management		Endpoint certificate	
Access Control Management		Physical security keys	
Access Control Management	10.3.2	Irrespective of a user's location, we require multi-factor authentication for access to our most critical or sensitive data or systems.	Yes
Access Control Management	10.3.3	We require multi-factor authentication for all remote login access to the corporate network (e.g., Virtual Private Network (VPN), Remote Desktop Protocol (RDP), or other secure remote access, etc.).	Yes
Access Control Management	10.3.4	Irrespective of a user's location, we require multi-factor authentication and encrypted channels for all administrative account access.	Yes
Network Infrastructure Management	**Firewall**		
Network Infrastructure Management	11.1.1	The organization configures firewalls to prevent unauthorized access, and the firewall configurations are reviewed at least annually.	Yes
Network Infrastructure Management	11.1.2	Our formal firewall policy is to deny-all by default, permit-by-exception to ensure only explicitly approved incoming/outgoing traffic is permitted.	Yes
Network Infrastructure Management	**Wireless Network Security**		

Area	Sr.No	Question	Bank RESPONSE
Network Infrastructure Management	11.2.1	We implement wireless security policies and protocols that require strong encryption standards.	Not Applicable.No Wireless devices/connections are used in Canara Bank Network
Network Infrastructure Management	11.2.2	Our organization maintains a completely separate (logically or physically) wireless network for guests, Bring Your Own Device (BYOD) users, and other untrusted devices.	Not Applicable.No Wireless devices/connections are used in Canara Bank Network
Network Infrastructure Management	**Network Segmentation**		
Network Infrastructure Management	11.3.1	In our organization, the network is segmented based on: (select the answer(s) that best reflects your network segmentation approach):	Yes
Network Infrastructure Management		Business unit	Yes
Network Infrastructure Management		Geographic/regional	Yes
Network Infrastructure Management		Classification level of the information stored on the servers	Yes
Network Infrastructure Management		Data processing and storage based on the sensitivity of the data	Yes
Network Infrastructure Management		Isolating critical systems, functions, or resources	Yes
Network Infrastructure Management		Role and functionality	Yes
Network Infrastructure Management	11.3.2	To mitigate risks/threats and increase our operational resilience, we implement enhanced security controls/protections (select all that apply):	
Network Infrastructure Management		Perform traffic filtering between network segments.	Yes
Network Infrastructure Management		Use network appliances to filter ingress or egress traffic and perform protocol filtering.	Yes
Network Infrastructure Management		Deploy a network intrusion prevention solution to block known malicious traffic at network boundaries.	Yes
Network Infrastructure Management		Implement port-level access control utilizing 802.1x or similar Network Access Control (NAC) protocols for authenticating and authorizing device.	Yes
Network Infrastructure Management		Configure software on user workstations, with a default-deny rule to drops all traffic except those services and ports that are explicitly allowed.	Yes
Malware Defenses	**Malware Protection**		
Malware Defenses	12.1.1	The organization implements the following malware protections:	
Malware Defenses		Incoming emails are filtered/scanned for known malicious attachments and suspicious file types, including executable	Yes
Malware Defenses		Macro-enabled files cannot be run by default.	Yes
Malware Defenses		A quarantine service is provided.	Yes
Malware Defenses		Email attachments are evaluated in a sandbox to determine if malicious prior to delivery.	Yes
Malware Defenses		Emails are filtered to block suspicious messages based on their content or attributes of the sender.	Yes
Malware Defenses	12.1.2	The organization installs and regularly updates anti-malware solutions (e.g., anti-virus, anti-spyware, advanced endpoint security) to the following percentage of assets, and exceptions are documented.	
Malware Defenses		Workstations and laptops.	100% with exceptions documented
Malware Defenses		Servers, excluding hypervisor hosts.	100% with exceptions documented
Malware Defenses		Mobile devices, including tablets and phones but excluding laptops.	
Malware Defenses	12.1.3	Specify the endpoint security tool(s) used. If multiple, please add in commentary area.	

Area	Sr.No	Question	Bank RESPONSE
Malware Defenses		Solution provider name (e.g. "CrowdStrike, "Microsoft", or "VMware", etc.):	Yes
Malware Defenses		Solution/product name and included options ("Falcon Complete", "Microsoft Defender for Endpoint P2" or "Carbon Black EDR"):	Yes
Malware Defenses	12.1.4	The endpoint security tool(s) are configured to:(select all that apply)	
Malware Defenses		For those tools which require updated definitions, such tools are updating at least daily.	Yes
Malware Defenses		Block (as opposed to solely notify of) suspected malicious processes and files.	Yes
Malware Defenses		Find unmanaged assets, which are addressed at least weekly.	Yes
Malware Defenses		Enable anti-tamper features.	Yes
Continuous Vulnerability Management	**Vulnerability and Patch Management**		
Continuous Vulnerability Management	13.1.1	Vulnerability scans are performed at least	Quarterly
Continuous Vulnerability Management	13.1.2	Our organization deploys automated patch management processes/tools to update operating systems, software/applications, and other application software or firmware.	Yes
Continuous Vulnerability Management	13.1.3	Our organization deploys vulnerability patches:	Yes
Continuous Vulnerability Management	13.1.4	The organization's target timeframe to patch Common Vulnerability Scoring System (CVSS) v3 Critical Severity 9.0-10.0 vulnerabilities across your enterprise is:	15 days
Continuous Vulnerability Management	13.1.5	In the most recent full quarter, the organization was successful at achieving the target timeframe selected above in statement 13.1.4 to patch (select from list) CVSS Critical Severity vulnerabilities across the enterprise.	Yes.Bank is successful in achieving the target timeframe for CVSS Critical severity Vulnerabilities.
Continuous Vulnerability Management	13.1.6	The organization's target timeframe to patch Common Vulnerability Scoring System (CVSS) v3 High Severity 7.0-8.9 vulnerabilities across your enterprise is:	30 days
Continuous Vulnerability Management	**Penetration Testing**		
Continuous Vulnerability Management	13.2.1	In our organization, annual or more frequent penetration testing (i.e., testing that emulates adversary actions and hostile cyber attacks) is conducted on the network and critical systems.	Yes, the same is part of comprehensive VAPT which is conducted half yearly.
Continuous Vulnerability Management	13.2.2	Our processes require penetration testing activities that include, but are not limited to, the following: a) annual assessment(s) b) independent penetration agents simulate adversary actions c) testing scope includes the network and business critical systems/ applications d) penetration test results and recommendations are risk-rated and/or prioritized to mitigate or remediate vulnerabilities and weaknesses identified.	a) Yes b) Yes c) Yes d) Yes
Security Awareness and Skills Training	**Security Training**		
Security Awareness and Skills Training	14.1.1	In our organization, cybersecurity training is mandatory for all employees (select period from list).	Cyber security awarenes sessions is conducted to all IT staff, RO/CO staff on Quarterly basis. One Cyber security courses is mandated for all employees in our e-learning platform. Further we are conducting cyber security session for all the training programs of 3 days and above.
Security Awareness and Skills Training	14.1.2	Cybersecurity training is mandatory for vendors/contractors and third party partners with access to the corporate network (select period from list).	Cyber security awareness sessions for vendors are being conducted on half yearly basis.

Area	Sr.No	Question	Bank RESPONSE
Security Awareness and Skills Training	14.1.3	We perform an annual analysis to identify gaps in our cybersecurity skillset, and develop and implement training roadmaps and/or project plans to close identified gaps.	Yes, we nominate cyber security external training programs for the employees periodically based on the assessments.
Security Awareness and Skills Training	**Security Awareness Program**		
Security Awareness and Skills Training	14.2.1	Our cybersecurity awareness program materials train users to avoid common cyber-risks and threats, such as social engineering and phishing.	Yes
Security Awareness and Skills Training	14.2.2	We update cybersecurity awareness training and communications content frequently (at least annually) to embody the latest attack and social engineering techniques.	Yes
Security Awareness and Skills Training	14.2.3	Our organization tags external emails to alert employees that the email originated from outside the organization.	Yes
Security Awareness and Skills Training	14.2.4	The organization conducts internal phishing campaigns at least:	Monthly
Security Awareness and Skills Training	14.2.5	In the latest internal phishing campaign, the success ratio (% of employees that were successfully phished) was:	0.34%
Security Awareness and Skills Training	14.2.6	Our organization has a documented process to report suspicious emails to an internal security team to investigate.	Yes
Data Recovery	**Recovery Processes and Procedures**		
Data Recovery	15.1.1	Our organization conducts backups for **Applications**	Monthly
Data Recovery	15.1.2	Our organization conducts backups for **Databases**	Daily
Data Recovery	15.1.3	Our organization conducts backups for **Servers**	Monthly
Data Recovery	15.1.4	Our organization conducts backups for **Workstations/laptops and endpoints**	As and when requested
Data Recovery	15.1.5	Our organization conducts backups for **Critical Information** (Critical Information means critical information as defined by the organization's information classification or business continuity / disaster recovery plans/policies)	Daily
Data Recovery	15.1.6	We test system restoration capabilities by performing a full restoration from a sample set of backup data at least.	Half-yearly
Data Recovery	15.1.7	To strengthen recovery from malicious encryption (e.g., crypto-ransomware attack) we:	
Data Recovery		Isolate backup files from the network (i.e., backup files are not continuously accessible from the network).	Yes
Data Recovery		Store offline (archive) backups onsite.	Yes
Data Recovery		Store offline (archive) backups offsite.	Yes
Data Recovery		Backups are immutable (i.e., cannot be altered or deleted)	Yes
Data Recovery	15.1.8	After an incident is contained, the organization implements procedures/processes to remediate affected systems and restore systems to our normal or fully operational state.	Yes
Data Recovery	**Business Continuity**		
Data Recovery	15.2.1	The organization maintains a business continuity/disaster recovery plan, and the plan is tested:	Quarterly/Half Yearly/Annually
Data Recovery	15.2.2	The organization's Recovery Time Objective (RTO), defined as the maximum target period IT functionality may be lost due to an incident, is the following for critical systems:	Less than 3 hours
Data Recovery	15.2.3	Our organization reviews and updates IT disaster recovery plans to address system/organizational changes, lessons learned, or problems encountered during the most recent restoration.	Annually

Area	Sr.No	Question	Bank RESPONSE
Data Recovery	15.2.4	The organization maintains an alternate backup IT facility which would be categorized as:	Yes. Tier IV DR
Data Recovery	15.2.5	The organization has the capability to immediately failover to redundant or standby information systems.	Yes
Data Recovery	15.2.6	We review and revise IT disaster recovery plans on an annual basis; revisions incorporate lessons learned from IT disaster recovery plan tests and previous restoration activities.	Yes
Service Provider Management	**Outsourced Services**		
Service Provider Management	16.1.1	The organization conducts security assessments and periodic re-assessments on third party partners and other service providers with access to information assets.	Yes
Service Provider Management	16.1.2	The organization reviews independent audit reports (e.g., SSAE 18 SOC 2, HITRUST certification, or Standardized Information Gathering (SIG), Agreed Upon Procedures (AUP)*) from third party partners and other service providers with access to information assets at least annually. * The most recent version of the standards listed.	Yes
Service Provider Management	16.1.3	Our organization requires confirmation from our cloud vendors that they are compliant with any applicable laws related to data storage and data transfer.	Yes
Service Provider Management	16.1.4	Our cloud provider utilizes DDoS mitigation solutions.	Yes
Service Provider Management	**Third Party Risk Management Oversight**		
Service Provider Management	16.2.1	Our organization requires vendors to maintain insurance or another means of indemnification for losses caused by the provider, including from a privacy breach.	Yes
Service Provider Management	16.2.2	The organization requires interconnection agreements for connections between the organization's network and external networks (e.g., third-parties, vendors, etc.).	Yes
Service Provider Management	16.2.3	If interconnection security agreements are required, the organization's agreements contain information/cybersecurity requirements including risk-based monitoring for anomalous activities.	Yes
Service Provider Management	16.2.4	The organization has a process or technical solution to identify, assess, manage, monitor, and reduce the risks from third party partners and other service providers.	Yes
Service Provider Management	16.2.5	We maintain an inventory of what percentage of third party or vendor managed information systems (residing outside of the organization's boundaries and not under the organization's direct control) that have access to or process our information assets (e.g., cloud, SaaS, etc.).	Yes
Incident Response Management	**Incident or Breach Response Plan(s)**		
Incident Response Management	17.1.1	Our incident response or breach response plan is (select all that apply):	
Incident Response Management		Formally documented.	Yes
Incident Response Management		Aligned with the National Institute of Standards and Technology (NIST) Special Publication 800-61.	Yes
Incident Response Management		Aligned with ISO/IEC 27035 guidance	Yes
Incident Response Management		Aligned with an other governmental authority (e.g. CERT or ANSSI) – please describe in comments.	Yes

Area	Sr.No	Question	Bank RESPONSE
Incident Response Management	17.1.2	Our incident response program requires incident response and reporting instructions within contracts for third party partners or service providers that manage or have access to corporate/organizational data via contract riders or agreed-upon terms and conditions.	Yes
Incident Response Management	17.1.3	We have internal resources and/or an active contract with incident response service providers to accomplish incident containment, eradication (e.g., eliminate malware and return systems to normal operations), and orchestrate recovery.	Yes
Incident Response Management	17.1.4	Our incident response strategy is integrated with organization/corporate business continuity plans and IT disaster recovery capabilities.	Yes
Incident Response Management	17.1.5	Our incident response program encompasses the following core capabilities:	
Incident Response Management		Processes/procedures for performing incident classification, prioritization, handling, reporting, and recovery.	Yes
Incident Response Management		Ransomware response playbook.	Yes
Incident Response Management		Playbook for a ransomware incident of 3rd parties/MSPs.	Yes
Incident Response Management		A defined response team structure.	Yes
Incident Response Management		Plan testing or exercise requirements.	Yes
Incident Response Management		Plan review and update schedule.	Yes
Incident Response Management		Process to resume business operations by restoration of known clean backups	Yes
Incident Response Management		Process/procedures for recovery, such as activating the IT disaster recovery plan	Yes
Incident Response Management		Names and contact information for relevant authorities, including law enforcement	Yes
Incident Response Management	17.1.6	We review and revise incident/breach response plans to address system/organizational changes, lessons learned, or problems encountered during previous incident detection and response activities.	Annually
Incident Response Management	**Incident Response Exercises**		
Incident Response Management	17.2.1	Our organization conducts incident/breach response scenario-based exercises that: (select all that apply)	
Incident Response Management		Include Cyber Incident response tabletop reviews.	Yes
Incident Response Management		Requires participation from cyber incident response and senior management personnel defined in our plan to refresh their responsibilities.	Yes
Incident Response Management		Reflect current threats and risks faced by our industry or similar organizations, including facing threats from ransomware actors.	Yes
Incident Response Management		Results in documentation of lessons learned and revisions/improvements required.	Yes
Incident Response Management	17.2.2	Our organization conducts cyber incident/breach response scenario-based exercises at least:	Quarterly
Incident Response Management	**Incident Containment and Mitigation Activities**		
Incident Response Management	17.3.1	What is the Applicant's average time to triage and contain security incidents of workstations for the most recent completed quarter?	No incidents reported in the previous year.
Incident Response Management	17.3.2	Our incident monitoring/ handling practices require incident documentation	Yes

Area	Sr.No	Question	Bank RESPONSE
Incident Response Management	**Recovery Communications**		
Incident Response Management	17.4.1	We have a documented crisis communication plan that addresses communications activities such as, but not limited to, the following: a) emergency contact information for senior personnel, such as senior executives, corporate communications, the general counsel, and the CIO/CISO, etc. b) identification and contact information for key audiences, such as customer/ investor relations managers, employee unions, and state and federal regulators, etc.	Yes
Incident Response Management	17.4.2	Our crisis communication plan includes, but is not limited to: a) cyber insurance policy documentation and contact information b) guidelines and procedures for establishing a corporate spokesperson c) approval and escalation procedures to clear information or press releases prior to external release d) breach notification template and consultation process with external legal counsel to review and approve notices prior to release	Yes
Incident Response Management	17.4.3	In concert with our incident/ breach response plans, we maintain pre-negotiated contracts with data breach response/ resolution providers (e.g., call centers, notices and communications, and credit monitoring services).	Yes
Technology in Use	**Microsoft 365 Protections**		
Technology in Use	18.1.1	The organization uses Microsoft 365.	Yes
Technology in Use	18.1.2	The organization uses the following protections with Microsoft 365.	
Technology in Use		Microsoft 365 Advanced Threat Protection.	Yes
Technology in Use		Multi-Factor Authentication is required at all times.	Yes
Technology in Use		Other (please describe email security capabilities in	DKIM,SPM,DMARC,Anti-Phishing etc.
Technology in Use		Not applicable.	
Technology in Use	**Cloud Utilization**		
Technology in Use	18.2.1	The organization utilizes cloud computing in the following way(s): *(please check all that apply)*	
Technology in Use		Public cloud	Yes
Technology in Use		Private cloud	Yes
Technology in Use		Hybrid of public/private cloud	Yes
Technology in Use		The organization does not utilize cloud computing	
Technology in Use	18.2.2	Please describe the types of business processes, applications or functions which the organization relies on for cloud computing.	Chatbots, Banking services though Whatsapp, Video KYC application, Business application to host internal sites, Power Bi for dashboard requirements etc.
Technology in Use	**Information / Cybersecurity Capabilities and Tools**		
Technology in Use	18.3.1	The organization operates the following Information Technology (IT) and Information/Cybersecurity tools and capabilities *(please check all that apply and indicate key vendors)*:	
Technology in Use		Network Intrusion Detection/Prevention Systems (IDPS)	Yes
Technology in Use		Unified Threat Management (UTM)/ Threat Prevention/ Protection Systems (TPS)	Yes

Area	Sr.No	Question	Bank RESPONSE
Technology in Use		Network Data Loss Prevention (DLP) solution	Yes
Technology in Use		Protective Domain Name Service (PDNS)	Yes
Technology in Use		Security Information and Event Management (SIEM)	Yes
Technology in Use		Email DLP solution	Yes
Technology in Use		Enforce Sender Policy Framework (SPF)	Yes
Technology in Use		DomainKeys Identified Mail (DKIM)	Yes
Technology in Use		Domain-based Message Authentication, Reporting and Conformance (DMARC)	Yes
Technology in Use		Block malicious and phishing URLs	Yes
Technology in Use		Multi-Factor Authentication to on-premise backups	Yes
Technology in Use		Multi-Factor Authentication to cloud-based backups	Yes
Technology in Use		Host Intrusion Prevention Systems (HIPS)	Yes
Technology in Use		File Integrity Tools (Allowlisting)	Yes
Technology in Use		Endpoint DLP solution	Yes
Technology in Use		Endpoint Detection and Response (EDR) solutions	Yes
Technology in Use		Advanced Endpoint Security	Yes
Technology in Use		Network Detection and Response (NDR) solutions	Bank is using NBAD for Network Detection & Response.
Technology in Use		Identity and Access Management solutions	Yes
Technology in Use		Bring Your Own Device (BYOD) security solutions	Yes
Technology in Use		Password management software	Bank uses A Privileged Identity Management (PIM) solution to securely access and manage critical server passwords.
Technology in Use		Wireless Network Security solutions	Not Applicable
Technology in Use		Network Intrusion Detection Systems (NIDS)	Yes
Technology in Use		DDoS mitigation solutions	Yes
Technology in Use		Please describe other tools or capabilities that support the organization's cyber/information security program	Multiple solutions are implemented that strengthen the Cyber Security of the Bank, which include SIEM, PIM, DLP, NBAD, Anti-DDoS solution,VA, UEBA, SOAR+TIP, EDR, Anti-APT, PCAP, DAST, SSLi decryptor, Load Balancer & services like BAS, Threat Intel services, Cyber Range, DDoS Drill.
Event History	**Event History**		
Event History	19.1.1	Within the past 5 years, has the organization sustained any network security incidents or data incidents that resulted in a material financial loss to the organization? If yes, please describe in detail below.	No
Event History	19.1.2	Within the past 5 years, has the organization received any demands or claims relating to allegations of theft of information or breach of information security? If yes, please describe in detail below.	No

Area	Sr.No	Question	Bank RESPONSE
Event History	19.1.3	Within the past 5 years has the organization been required to notify any individuals or entities because of a breach of information security? If yes, please describe in detail below.	No
Event History	19.1.4	Within the past 5 years, has the organization been the subject of any government action, regulatory investigation or subpoena regarding any alleged violation of any privacy/data security law or regulation? If yes, please describe in detail below.	No
Event History	19.1.5	Within the past 5 years, has the organization experienced a network outage, or substantial loss of IT functionality for more than 6 hours? If yes, please describe in detail below.	No
Event History	19.1.6	Within the past 5 years has the organization sustained any network security incidents, or outages as the result of the actions of a 3rd party vendor (e.g. cloud vendors, IT consultants, payroll, data	No
PCI	**PCI**		
PCI	22.1.1	Your organization is required to be compliant with Payment Card DSS Standards (PCI-DSS).	Yes we have obtained necessary certificates from the vendors.
PCI	22.1.2	Revenue for credit card transactions that are processed annually through the organization's system:	Total Revenue (Inc GST) (April-September 2025): Interchange Income - Rs.56,48,96,005.29
PCI	22.1.3	Percentage of these transactions completed online or other card not present transactions vs. Point of Sale (POS) transactions:	POS Txns : 63.90% of Total Txns . Ecomm Txns : 33.69% of Total Txns
PCI	22.1.4	Percentage of revenue completed by online or other card not present transactions vs. Point of Sale (POS) transactions:	Bifurcation not available
PCI	22.1.5	PCI Merchant Level (i.e., 1-4):	Level 4
PCI	22.1.6	The organization is currently compliant with PCI-DSS Validation Requirements as required by your merchant level (i.e. Level 1 - 4).	Yes
PCI	22.1.7	Version of PCI-DSS against which the organization was assessed:	Version 4.0.1

Area	Sr.No	Question	Bank RESPONSE
PCI	22.1.8	Percentage of the organization's POS System that is EMV compliant (100%, 75%, 50%, 25%, 0%):	100%
PCI	22.1.9	The organization's POS system was installed with the assistance of a system integrator, reseller or consultant qualified by the PCI Security Standards Council Qualified Integrators and Resellers (QIR) program.	Yes
PCI	22.1.10	The organization maintains a separate network for their POS system (e.g. through the use of jump servers).	Not Applicable
PCI	22.1.11	The organization require third party providers, who operate or maintain your POS system, to maintain insurance or another means of indemnification for loss caused by the provider	Yes
PCI	22.1.12	The organization utilizes a payment processor that provides regular evidence of PCI-DSS compliance.	Yes
PCI	22.1.13	Any PCI data that is stored is encrypted while at rest.	Yes
PCI	22.1.14	Any PCI data that is stored is in tokenized form while at rest.	Yes
PCI	22.1.15	The organization implements malware protection on their POS terminals.	Yes
PCI	22.1.16	The organization implements log monitoring around PCI and POS system activity.	Yes
PCI	22.1.17	Intrusion Detection Systems (IDS) and Data Loss Prevention (DLP) are implemented within the POS network and any other PCI systems.	Yes
PCI	22.1.18	Penetration testing and vulnerability scans are performed on the POS network and any other PCI systems at least annually.	Yes
PCI	22.1.19	IDS and DLP are monitored 24 hours a day.	Yes
PCI	22.1.20	PCI data is either encrypted or tokenized while transit.	Yes
PCI	22.1.21	The organization utilizes Point to Point Encryption (P2PE) that is PCI-DSS certified.	Yes
PCI	22.1.22	In addition to having P2PE that is PCI-DSS certified, the organization does not hold the decryption keys for the PCI data, and PCI data may only be decrypted in a third party provider's environment.	Yes
PCI	22.1.23	The organization utilizes PCI Validated P2PE, approved by the PCI Security Standard Council.	Yes
PCI	22.1.24	The organization is compliant with the Song Beverly Act and other similar laws/regulations.	Yes
PCI	22.1.25	The organization is compliant with the credit card display provisions of the Fair and Accurate Credit Transaction Act (FACTA).	Yes

Overseeing Executive

Date 05.01.2026