Internal

केनरा बैंक Canara Bank
भारत सरकार का उपक्रम A Government of India Undertaking
सिंडिकेट Syndicate

Ref: SD: 416/417/11/12:2025-26 **December 29, 2025**

The Vice President **BSE Limited** **Phiroze Jeejeebhoy Towers** **Dalal Street** **Mumbai - 400 001** Scrip Code: **532483**	**The Vice President** **Listing Department** **National Stock Exchange of India Ltd** **Exchange Plaza** **Bandra-Kurla Complex, Bandra [E]** **Mumbai - 400051** Scrip Code: **CANBK**

Subject: Compliance Certificates and Reports on Securities Exchange Board of India-Cybersecurity and Cyber Resilience Framework (SEBI-CSCRF).

Dear Sir/Madam,

In terms of SEBI Circular No. SEBI/HO/ ITD-1/ITD CSC EXT/P/CIR/2024/113 dated August 20, 2024, please find enclosed herewith Certificates of Compliance and Reports on Securities Exchange Board of India - Cybersecurity and Cyber Resilience Framework (SEBI-CSCRF).

This is for your information and records.

Yours faithfully,

Internal

Santosh Kumar Barik
Company Secretary

प्रधान कार्यालय
112, जे सी रोड, बेंगलूरु - 560002
E-Mail - hosecretarial@canarabank.com

Head Office
112 J C Road, Bengaluru - 560002
www.canarabank.com

F +91 80 22248831
T +91 80 22100250

Internal

Internal

केनरा बैंक Canara Bank

सिंडिकेट Syndicate

Together We Can

Annexure-A : VAPT Report

Name of the Organization: Canara Bank

Entity Type: Bank

Entity Category: Qualified Regulated Entity (Qualified RE).

Rationale for the Category: Canara Bank is registered under multiple licenses with SEBI and their classifications as per SEBI CSCRF are as Depository Participant (DP)- Qualified RE, Merchant Banker and Proprietary Stock Broker- small size RE and Bankers to an Issue (BTI) and Self-Certified Syndicate Banks (SCSBs).
As per SEBI CSCRF guidelines, where a Regulated Entity falls under multiple classifications, the compliance requirements applicable to the highest classification shall prevail. Since the Bank holds Depository Participant (DP) registration, which falls under the Qualified Regulated Entity (Qualified RE) classification, Canara Bank is accordingly classified under Qualified RE.

Period of Audit: 01.10.2025 - 17.11.2025.

Name of the Auditing Organization: M/s AKS IT Services Pvt. Ltd.

Date on which Cyber Audit Report presented to IS Committee: 17.11.2025

Internal

Authorized signatory declaration:

I hereby confirm that the information provided herein is verified by me and I shall take the responsibility and ownership of this VAPT report.

Signature:

Name of the signatory: K Satyanarayana Raju

Designation: MD-CEO

Company stamp:

केनरा बैंक CANARA BANK MD & CEO's SCRT. H.O., BENGALURU-2

Annexures:

1. Minutes of the Meeting (MoM) of Information Security Committee dated 17.11.2025 in which the cyber audit report was approved.

2. VAPT report as submitted by the auditor.

Confidential

Internal

Internal

केनरा बैंक Canara Bank

Syndicate

Together We Can

Table of Contents

Internal

Confidential

Internal

Internal

केनरा बैंक Canara Bank Syndicate Together We Can

1. **Auditor's Declaration**

TO WHOM SO EVER IT MAY CONCERN

This is to declare and certify that I am an Employee of firm M/s AKS IT Services Pvt. Ltd. with CERT-In empanelment 21 October 2024 to 31 October 2027. I have conducted VAPT for Canara Bank for half year period April-September 2025 as per the requirements of SEBI. The scope of VAPT covers following circulars/ guidelines/ advisories issued by SEBI:

Checklist for VAPT compliance as required:

#	Area	Details (assets, applications, etc.) of the Audit area	Is the Entity Compliant? (Yes / No)	Auditor's comments
1.	Vulnerability Assessment (VA)	• DP Secure • FOC • ASBA • UAT ASBA • Servers • Appliances • Network Devices	Yes	Conducted VA for the mentioned assets and shared assessment report with the Bank
2.	External Penetration Testing (PT)	• DP Secure • FOC • ASBA • UAT ASBA	Yes	Conducted External PT for mentioned assets and shared assessment report with the Bank
3.	Wi-Fi Testing	NIL	Not Applicable	As the scope of assets are not utilizing Wi-Fi, hence Wi-Fi testing is not applicable.
4.	API Security Testing	1 API with 4 end points	Yes	Conducted API security Testing for mentioned assets and shared assessment report with the Bank
5.	VA and PT of mobile applications	NIL	Not Applicable	There are no mobile applications under the scope, hence VA and PT of mobile applications is not applicable
6.	Network segmentation testing	**In-Scope:** VLAN IDs - 2, 7, 838,73,122, 83,216, 669,659,950,951, DRC,52,51,90,822,	Yes	Conducted Network Segmentation Testing for In-Scope SEBI segments from Out-of-Scope

Internal

Internal

केनरा बैंक Canara Bank
Together We Can

CSCRF-Annexure-A

#	Area	Details (assets, applications, etc.) of the Audit area	Is the Entity Compliant? (Yes / No)	Auditor's comments
		669,659,950,951, DRC,52,51,90,822, 194,707,97,166, 718,812,102,106, 88,817,109,839, 701,710,813,704, 825,823. **Out-of-Scope:** VLAN IDs-Default VLAN1 and 222		SEBI segments and shared assessment report with the Bank. The out-of-scope segments through which the testing was conducted is as mentioned in adjacent column.
7.	OS and DB Assessment	01-Data base 103 - Servers	Yes	Conducted DB assessment for mentioned asset and shared assessment report with the Bank. OS assessment is conducted as part of configuration audit.
8.	VAPT of cloud implementation	NA	Not Applicable	There are no cloud assets in the scope, hence VAPT of cloud implementation is not applicable.
9.	Configuration audit	• Servers • Appliances • Network Devices	Yes	Conducted Configuration audit for mentioned assets and shared assessment report with the Bank

Internal

I confirm that the VAPT has been conducted as per the auditor's guidelines prescribed in this framework.

I also confirm that I have no conflict of interest in undertaking the above-mentioned activities.

For and on behalf of **M/s AKS IT Services Pvt. Ltd**

Name: Lt Cdr Akash Mahindrakar (Retd.)
Contact no.: +91 9766264616
Place: Noida
Date:18.12.2025

AKASH MAHINDRAKAR

Digitally signed by AKASH MAHINDRAKAR
Date: 2025.12.18 19:10:46 +05'30'

Confidential

Internal

Internal

2. **Executive Summary:**

As part of compliance with SEBI Cyber Security and Cyber Resilience Framework (CSCRF), M/s AKS IT Services Private Limited conducted the Vulnerability Assessment and Penetration Testing (VAPT) in accordance with the Annexure-2 VAPT format prescribed under SEBI CSCRF.
The assessment covered the defined scope of assets related to SEBI activities.
The following is the consolidated summary of all the assessments.
Critical: 54, High :107, Medium:5720 and Low:594.

3. **Scope of VAPT**

S. No.	Type of Assessment	List the details of the assessment
1.	Vulnerability Assessment of Infrastructure - Internal and External	147 IPs
2.	Vulnerability Assessment of Applications - Internal and External	**04-Applications** • DP Secure - 1 Application • FOC - 1 Application • ASBA - 1 Application • UAT ASBA - 1 Application
3.	External Penetration Testing - Infrastructure and Applications	**04-Applications** • DP Secure - 1 Application • FOC - 1 Application • ASBA - 1 Application • UAT ASBA - 1 Application
4.	Wi-Fi Testing	Not Applicable
5.	API Security Testing	**1 API with 4 end points** • inquireCasaAccountBalance • asbaPANValidation • partialEarmarkFunds • partialReleaseEarmark
6.	Network Segmentation Testing	34 Segments
7.	VA and PT of Mobile Applications	Not Applicable
8.	OS and DB Assessment	01 Oracle Database
9.	VAPT of Cloud implementation and Deployments	Not Applicable
10.	Configuration audit	The following Operating Systems are being covered for configuration audit. Oracle Solaris 11, Cisco NX-OS, Cisco IOS XE, Check Point Firewall, Gaia OS, Fortigate OS Juniper OS, Windows server 2016, 2019 and 2022.

Internal

Internal

4. **Tools used:**

   4.1. **Name of the Tool:** Burpsuite Professional, Tenable, Nessus, Postman, Nmap, SQLMap
   4.2. **Type:** Commercial / Open-Source
   4.3. **Operations:** Both

5. **Exclusions, if any:** NIL

Internal

Internal

Internal

6. Summary of the VAPT Report:

6.1. Details of Vulnerability Assessment findings:

S.No.	Vulnerability Assessment Findings Details											
1.	Auditor (Name) for VA:	Mr. Vivek Krishna Das, Mr. Abhishek Bhoi, Mr. Vaibhav Verma										
2.	VA Start Date:	01.10.2025										
3.	VA End Date:	17.11.2025										
4.	Scope	Vulnerability Assessment										Auditor Remarks
5.		Number of Identified vulnerabilities					Closure Timelines	Open vulnerabilities					
6.		Critical	High	Medium	Low	Total		Critical	High	Medium	Low	Total	
7.	Critical Assets	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NIL
8.	VA of infrastructure - Internal and External	54	104	176	9	343	17.03.2026	54	104	176	9	343	Conducted as per SEBI CSCRF
9.	VA of Applications - Internal and External	0	0	4	10	14	17.03.2026	0	0	4	10	14	Conducted as per SEBI CSCRF
10.	Wi-Fi Testing	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NIL
11.	API Security Testing	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NIL
12.	Network Segmentation	0	0	10	2	12	17.03.2026	0	0	10	2	12	Conducted as per SEBI CSCRF
13.	VA of mobile applications	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NIL
14.	OS and DB Assessment	0	0	51	41	92	17.03.2026	0	0	51	41	92	Conducted as per SEBI CSCRF

Internal

Internal

15.	VA of cloud deployments	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NIL
16.	Configuration Audit	0	0	5479	531	6010	17.03.2026	0	0	5479	531	6010	Conducted as per SEBI CSCRF
17.	Others, please specify												

Internal

Internal

Internal

6.2. Details of Penetration Testing findings:

S.No.	Penetration Testing Findings Details											
1.	Auditor (Name) for PT:	Mr. Vivek Krishna Das, Mr. Abhishek Bhoi, Mr. Vaibhav Verma										
2.	PT Start Date:	01.10.2025										
3.	PT End Date:	17.11.2025										
4.	Scope	Penetration Testing										Auditor Remarks
5.		Identified vulnerabilities					Closure Timelines	Open vulnerabilities				
6.		Critical	High	Medium	Low	Total		Critical	High	Medium	Low	Total
7.	Critical Assets	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NIL
8.	External Penetration Testing - Infrastructure and Application	0	3	0	0	3	17.03.2026	0	3	0	0	3	Conducted as per SEBI CSCRF
9.	PT of mobile applications	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NIL
10.	PT of cloud deployments	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NIL
11.	API Security Testing	0	0	0	1	1	17.03.2026	0	0	0	1	1	Conducted as per SEBI CSCRF
12.	Others, please specify												

Internal

Internal

Internal

7. **Detailed Report**- Shared with Bank.

8. **Risk Rating description**

Rating	Description
CRITICAL	The failure has an impact on the system delivery resulting in outage of services offered by the RE.
HIGH	Represents weakness in control with respect to threat(s) that is/are sufficiently capable and impacts asset (s) leading to regulatory non-compliance, significant financial, operational and reputational loss. These observations need to be addressed with utmost priority.
MEDIUM	Represents weakness in control with respect to threat(s) that is/are sufficiently capable and impacts asset (s) leading to exposure in terms of financial, operational and reputational loss. These observations need to be addressed within a reasonable timeframe.
LOW	Represents weaknesses in control, which in combination with other weakness can develop into an exposure. Suggested improvements for situations not immediately/directly affecting controls.

Internal

Internal

Internal

केनरा बैंक Canara Bank

Cyber Security Wing, Head Office, Bangalore

Minutes of Meeting (MOM) of Information Security Committee held on 17.11.2025

Information Security Committee Chairman:

1. Shri. S K Majumdar, Executive Director

Information Security Committee Member Secretary & Convener:

1. Shri. A Ramesh babu, General Manager & CISO, CS Wing

Information Security Committee Members:

1. Shri. Purshottam Chand, Chief General Manager, Treasury Wing
2. Shri. Alok Kumar Agarwal, Chief General Manager, TS Wing
3. Shri. Dilli babu, General Manager, DBS Vertical, TS Wing
4. Shri. Amit Mittal, GCFO, General Manager, FM Wing
5. Shri. Adish Yadav, General Manager, RM Wing
6. Shri. Papanasam S, DPO, Deputy General Manager, S&DA Vertical, SR&GS Wing
7. Shri. Capt. Abhishek Srivastava, CSO, Divisional Manager, GA Wing

Participants Present:

1. Shri. S K L Das, General Manager, CPVM Vertical, TS Wing
2. Shri. T V Krishna Mohan, General Manager, TM Vertical, Operations Wing
3. Shri. Manoj Kumar, General Manager, Resources Vertical, SR&GS Wing
4. Shri. Rajesh R, General Manager, C&PC Vertical, TS Wing
5. Shri. Shreenath Joshi, General Manager, CLO, General Manager, CIBL, HR&PR Wing
6. Shri. Sudhakar Kotary, CP Vertical, Operations Wing
7. Smt. Muthulakshmi P, General Manager, CS Vertical, Operations Wing
8. Shri. Avinash Purohit, Deputy General Manager, IT Vertical, TS Wing
9. Shri. Vikas Mehta, Deputy General Manager, TO Vertical, TS Wing
10. Shri. Satyabrat Maharana, Asst. General Manager, CS Wing
11. Shri. Vadiraj S Kulkarni, Asst. General Manager, CS Wing
12. Shri. N Praveen Babu, Asst. General Manager, CS Wing
13. Shri. Keshav Kumar, Director, NCIIPC South

Internal

Shri. A Ramesh Babu, CISO, General Manager, CS Wing, Convener of the Committee welcomed the information Security Committee Chairman, members, and other participants and briefed about the agenda to be discussed in the meeting.

Internal

Internal

Agenda
Status on Compliance Audit of SEBI CSCRF

1. **Background:**

   On August 20, 2024, SEBI has formulated Cybersecurity and Cyber Resilience Framework (CSCRF) for its Regulated Entities (REs) to ensure adequate cyber resiliency.

2. **Discussion:**

- The CISO informed the committee that the SEBI CSCRF compliance audit was conducted by a Cert-In empanelled auditing firm and the final Cyber Audit Report (Annexure-A), SOC Efficacy (Annexure-N) Report has been submitted to the committee for the perusal.
- At present, as per our SEBI licenses, our Bank falls under the Qualified Regulated Entity (QRE) category, since our DP license (DP Secure package) is classified under QRE as per SEBI CSCRF. This pertains to the e-Syndicate Bank and as per the Board's directions, no DP operations are being carried out. Existing DP accounts (around 1500) related to ex-staff and staff are being closed or transferred as there are no operations.
- One pending point for SEBI CSCRF compliance audit is the implementation of the Automated Cyber Capability Index (CCI) tool. However, as per SEBI CSCRF, CCI report to be submitted annually and the submission not falls under this half year cycle.
- Our Bank currently does not have this automated Cyber Capability Index (CCI) tool and is in the process of exploring the same for implementation. A tentative timeline of 31.03.2026 has been set, this may be extended depending on industry readiness. Meanwhile, the CCI report has been prepared manually and presented to the auditor.
- Our subsidiary M/s CanBank Securities Limited (CBSL) holds NSDL license and our bank's DP license is with CDSL. Currently the process for obtaining the CDSL license by CBSL is currently underway. CBSL has submitted the application to CDSL, and the license approval is in progress.
- Once the CDSL license is obtained by CBSL, the DP accounts will be transferred to CBSL and the Bank will transfer the existing DP accounts to CDSL and will surrender its DP license. Consequently, the Bank will fall under the Small Size RE category, where complied with SEBI CSCRF compliance and Qualified RE requirements will no longer be applicable.
- The CISO further updated the committee that mandatory reports– Cyber Audit Report, SOC Efficacy Report and VAPT Report are required to be submitted to SEBI, NSE/BSE, and CDSL as per regulatory guidelines. Preparation of the detailed VAPT report is currently in progress and the final consolidated report will be submitted upon completion.
- All applicable reports will be submitted to SEBI and other respective agencies with the signature of the MD & CEO, and the submissions will be completed within this December 2025 month.

3. **Committee after deliberations:**

   The Committee deliberated and noted the contents of the above note.

A Ramesh Babu
General Manager & CISO

Internal

Internal

Annexure-B: CSCRF Cyber Audit Report

Name of the Organisation: Canara Bank

Entity Type: Bank

Entity Category: Qualified Regulated Entity (Qualified RE).

Rationale for the Category: Canara Bank is registered under multiple licenses with SEBI and their classifications as per SEBI CSCRF are as Depository Participant (DP)- Qualified RE, Merchant Banker and Proprietary Stock Broker- small size RE and Bankers to an Issue (BTI) and Self-Certified Syndicate Banks (SCSBs).
As per SEBI CSCRF guidelines, where a Regulated Entity falls under multiple classifications, the compliance requirements applicable to the highest classification shall prevail. Since the Bank holds Depository Participant (DP) registration, which falls under the Qualified Regulated Entity (Qualified RE) classification, Canara Bank is accordingly classified under Qualified RE.

Period of Audit: 08th - 12th September 2025.

Name of the Auditing Organisation: M/s Control Case International Private Limited.

Date on which Cyber Audit Report presented to IS Committee: 17.11.2025.

Authorised signatory declaration:
I hereby confirm that the information provided herein is verified by me and I shall take the responsibility and ownership of this cyber audit report.
Further, this is to certify that:

a. Comprehensive measures and processes including suitable incentive / disincentive structures have been put in place for identification / detection and closure of vulnerabilities in the organization's IT systems.
b. Adequate resources have been hired for staffing our Security Operations Centre (SOC).
c. There is compliance by us with CSCRF.

Signature:

Name of the signatory: K Satyanarayana Raju

Designation: MD-CEO

Company stamp:

CANARA BANK MD & CEO's SCRT. H.O. BANGALURU-2

Annexures:

1. Minutes of the Meeting (MoM) of Information Security Committee dated 17.11.2025 in which the cyber audit report was approved.
2. Cyber audit report as submitted by the auditor.

Internal
Confidential

Internal

ControlCase
Compliance as a Service

TO WHOM SO EVER IT MAY CONCERN

This is to declare and certify that I am a Qualified Assessor of firm Control Case International Private Limited with CERT-In empanelment from till 31st October 2027. I have conducted Cyber audit for Canara Bank period April 1st 2025 to September 30th 2025 as per the requirements of SEBI.

Checklist for Cyber audit as required:

S. No.	Area	Details of the audit area	Is the Entity Compliant? (Yes / No)	Auditor's comments
1.	Cybersecurity and Cyber resilience policy	DP Secure, CITOS, Kondor Plus and ASBA	Yes	They have the Cybersecurity and Cyber resilience policy in Place
2.	Asset Inventory	DP Secure, CITOS, Kondor Plus and ASBA	Yes	Asset Inventory is in Place
3.	Risk assessment and Risk management	DP Secure, CITOS, Kondor Plus and ASBA	Yes	Risk assessment and Risk management is in place
4.	Supplychain risk management	DP Secure, CITOS, Kondor Plus and ASBA	Yes	Supplychain risk management is being performed
5.	Awareness and Training	DP Secure, CITOS, Kondor Plus and ASBA	Yes	Awareness and Training is being performed
6.	Data security	DP Secure, CITOS, Kondor Plus and ASBA	Yes	Data Security has been implemented
7.	Security continuous monitoring	DP Secure, CITOS, Kondor Plus and ASBA	Yes	Continuous Security Monitoring is in Place

ControlCase Confidential and Proprietary

Disclaimer: The update letter is issued at the request of the Client and should not be construed as substitute for Certificate or ROC/AOC/ROV, which will be released after successful completion of the process including Quality Assurance etc.

ControlCase International Pvt Ltd: Level 4 Corporate Center • Andheri-Kurla Road • Andheri (East) • Mumbai 400059, India

Phone: +91 22 66471800 • www.controlcase.com • *email:* contact@controlcase.com

Internal

Internal

Internal

ControlCase
Compliance as a Service

8.	SOC efficacy	DP Secure, CITOS, Kondor Plus and ASBA	Yes	SOC efficacy is in Place
9.	Incident Management and Response	DP Secure, CITOS, Kondor Plus and ASBA	Yes	Incident Management and Incident Response in Place
10.	Incident recovery planning	DP Secure, CITOS, Kondor Plus and ASBA	Yes	Incident Recovery Plan is in Place

I confirm that the audit has been conducted as per the auditor's guidelines prescribed in CSCRF (Cyber Audit).

I also confirm that I have no conflict of interest in undertaking the above-mentioned audit.

For and on behalf of Name: **Control Case International Private Limited.**

Internal

Name: **Vishal Naik**
Contact no.: **+912266741800**
Place: **Mumbai**
Date: **14th November 2025**

ControlCase Confidential and Proprietary

Disclaimer: The update letter is issued at the request of the Client and should not be construed as substitute for Certificate or ROC/AOC/ROV, which will be released after successful completion of the process including Quality Assurance etc.

ControlCase International Pvt Ltd: Level 4 Corporate Center • Andheri-Kurla Road • Andheri (East) • Mumbai 400059, India

Phone: +91 22 66471800 • www.controlcase.com • *email:* contact@controlcase.com

Internal

Internal

Internal

CANARA BANK

SEBI-Cyber Security and Cyber Resilience Framework

Internal

SEBI/HO/ ITD-1/ITD_CSC_EXT/P/CIR/2024/113 dated August 20, 2024,
SEBI/HO/ ITD-1/ITD_CSC_EXT/P/CIR/2025/119 dated, 28th August 2025

Internal

Internal

Statement of Confidentiality

This Confidential information is being provided to **CANARA BANK** as a deliverable of this assessment engagement. The sole purpose of this document is to provide you with the results of this engagement. Each recipient agrees that, before reading this document, it shall not distribute or use the information contained herein and any other information regarding ControlCase LLC for any purpose other than those stated.

Internal

Internal

Internal

Contents

Internal

Internal

Internal

1 Executive Summary

1.1 Introduction

ControlCase is a global provider of technology-driven compliance and security solutions. ControlCase is committed to partnering with clients to develop strategic information security and compliance programs that are simplified, cost-effective, and comprehensive in both on-premises and cloud environments. ControlCase provides the best experts, customer experience, and technology for regulations including PCI DSS, GDPR, SOC2, HIPAA, ISO 27001/2, CCPA, SWIFT, Microsoft SSPA, CSA STAR, SCA, PA DSS, PCI P2PE, PCI PIN, PCI 3DS, PCI Secure software, PCI Secure SLC.

ControlCase International Pvt. Ltd. is recognized as a CERT-In-empaneled IT Security Auditing Organization. ControlCase operates as a CERT-In-empanelled consulting and auditing organization, boasting CISA-certified auditors. The company has served over 100 clients in India, assisting them in adhering to RBI and CERT-In regulations such as DL-PSS, PAPG, BBPS, PPI, DPSC, CSF, Tokenization, and Data Privacy.

Moreover, ControlCase holds the designation of a QSA organization by PCI SSC, offering certification services for ISO/IEC 27001 and 27701 through the NABCB and RvA Accreditation body. With a client base exceeding 1000 across the US, CEMEA, Europe, and APAC regions, including over 50 banks, ControlCase has certified numerous banks and service providers.

Internal

This report pertains to the evaluation conducted on **CANARA BANK** from **8th September 2025 to 12th September 2025**. **CANARA BANK** contracted ControlCase International Pvt. Ltd. to conduct a system audit as per SEBI following guidelines.

SEBI Circular:

- **SEBI/HO/ ITD-1/ITD_CSC_EXT/P/CIR/2024/113 dated, 20th August 2024**
- **SEBI/HO/ ITD-1/ITD_CSC_EXT/P/CIR/2025/119 dated, 28th August 2025**

Internal

Internal

1.2 Scope of the Audit

The scope of the assessment is

- **DP Secure-Internal application currently not in active operation. Only the closure of existing accounts is in progress.**
- **ASBA**
- **CITOS & Kondor Plus**

1.3 List of SEBI Circular

S. No.	SEBI circular/ letter/ advisory	Issue date
1	SEBI/HO/ ITD-1/ITD_CSC_EXT/P/CIR/2024/113, SEBI/HO/ ITD-1/ITD_CSC_EXT/P/CIR/2025/119	August 20, 2024 August 28, 2025

1.4 List of all IT Infrastructure and Geographical location

Internal

S. No.	List of IT infrastructure/ Geographical locations/ Third-party vendors	Details (assets ID, asset name, applications, etc.) of the infrastructure assessed
1.	Infra of DP Secure	DP Secure
2.	Infra of ASBA	ASBA
3.	Infra od Treasury Applications (CITOS & Kondor Plus)	CITOS & Kondor Plus

Internal

Internal

1.5 Audit Approach

- **Scoping** – The assessor collaborated with the Client team to define the assessment scope and accurately determine the tier classification of the scoped application. This classification was agreed upon with the customer.
- **Assessment** – The assessor evaluated the application and related processes against the applicable CSCRF guidelines by:
  - Conducting interviews with Client stakeholders.
  - Performing process walkthroughs (e.g., application walk through, incident reporting, governance activities).
  - Reviewing documentation, including policies, procedures, and outputs from activities such as vulnerability management.
  - Conducting configuration reviews, including application assessments and hardening reviews.
- **Reporting** – Finally the assessor documented the findings in the SEBI-prescribed format.

1.6 Summary of Finding

S. No	Number of Non-conformities	Number of observations	Risk rating				Any other comments
			Critical	High	Medium	Low	
1	1	1	0	0	1	0	NA

Internal

Internal

Internal

1.7 Assessment Information

The engagement involved contributions from the following team members:

ControlCase Auditor	Canara Bank Team
Vishal Naik (CISSP Certificate No: 442782)  **Assessors:** Kamlesh Naidu Arjun K D	Amit Kumar Gupta M Rama Krishna B Shiva Chaitanya Navis Nayagam Vinoth Kumar Pratik G Krishna Chaitanya Laxmitosh Meera Pravin Mahajan

Internal

Report Date: 14th November 2025

Internal

Internal

2 Control-wise Compliance of SEBI-CSCRF

S. No	Standards prescribed by SEBI CSCRF (Clause number and text)	Description of Finding(s) / Observation(s)	Name of the system belongs to RE or third-party vendor	Status / Nature of findings	Risk rating (C/H/M/L) of the findings	C/I/A affected	Test cases used	Root Cause Analysis	Impact analysis	Auditor recommendations/ Corrective actions	Deadline of corrective action(s)	Management response	Whether similar issue was reported in the last three audits.	*List of documentary evidence including physical inspection/ sample size taken by the Auditor.
1	**GV.OC: Organizational Context:** The essential concomitants surrounding the REs' cybersecurity risk management decisions are understood. This includes mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements.	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	No	The assessor during the assessment, the auditor conducted interviews with relevant Canara Bank personnel, performed document reviews, and examined evidences supporting the Bank's cybersecurity governance and third-party risk management framework. The following documentary evidences were reviewed and verified to assess compliance with SEBI's requirement GV. OC: Organizational Context. Additionally, a sample size covering critical outsourced applications and vendors was selected for validation of the implemented controls and their effectiveness. **Documentary Evidences Reviewed:** 1. **IT Services Outsourcing Policy 2025–26.pdf** 2. **ASBA Vendor Agreement.pdf** 3. **DP Secure_Agreement.pdf** 4. **K+MASTER AGREEMENT.pdf** 5. **CITOS_SLA.pdf.** 6. **Canara Bank_Tata Consultancy Services_Vendor Risk Assessment Report_V1.1.pdf** 7. **Canara Bank_EXCELLEX TECHNOLOGIES_Vendor Risk Assessment Report_V1.1.pdf** 8. **Canara Bank_Oracle_Vendor Risk Assessment Final Report_V1.1.** 9. **Canara Bank_Finastra_Vendor Risk Assessment Final Report_V1.1.pdf** 10. **Email dated 7th August 2025** – Verified communication of cybersecurity objectives to relevant stakeholders for CITOS and Kondor+. 11. **VAPT Reports by AKS dated 29th October 2024 for CITOS and Kondor+** 12. **Information Security Policies_V7.5_FY 25–26_Section 6.1.1.pdf** 13. **CanaraBank_ASBA_Web-Application_Pentest_Report_v1.1_07_May_2025.pdf** 14. **System AUDIT REPORT AUDITOR REPORT.**
2	**GV. RR: Roles, Responsibilities and Authorities:** Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated.	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	No	The assessor conducted interviews with relevant Canara Bank personnel, reviewed documents, and examined evidences supporting the Bank's cybersecurity governance framework. It was confirmed that defined roles, responsibilities, and authorities are established, approved by management, and effectively communicated. The following evidences were reviewed to assess compliance with SEBI's requirement GV.RR: Roles, Responsibilities and Authorities, and a sample covering governance documents, awareness records, and access controls was verified for effectiveness.. **Documentary Evidences Reviewed:** 1. **Information Security Policy_V7.5_FY 25–26.pdf** 2. **ISC_Risk Assessment_March 2025.pdf** 3. **CYBERSECURITY POLICY_V.25_FY 2025–26.pdf**

Internal
Internal

Internal

														4. CISO Appointment Letter.pdf 5. CISO of the Bank.pdf 6. CYBER SECURITY WING BUDGET.pdf 7. NGSOC PO.pdf 8. ISG_V7.5_FY 25–26.pdf 9. ASBA Vendor Agreement.pdf 10. DP Secure_Agreement.pdf 11. K+MASTER AGREEMENT.pdf 12. CITOS_SLA.pdf 13. Mail Communication for Cybersecurity Awareness Session (IT-Tech Vertical) (1).pdf 14. Cyber Security Awareness Screenshots.docx 15. Consolidated List of Half-Yearly Cybersecurity Awareness – IT Staff – September 2025 (1).pdf 16. 17th September 2025 records from Privileged User Profile Register.pdf 17. Applications – User Access Request.pdf (dated August 2025)
3	**GV.PO: Policy:** Results of organization-wide cybersecurity risk management activities, performance, and outcomes are used to inform, improve, and adjust the risk management strategy.	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	No	The assessor during the assessment interviewed the Canara Bank Personnel and reviewed the Cyber Security Policy V2.5 FY 25–26 and noted that the Bank has a board approved and documented cybersecurity and cyber resilience policy outlining the framework for managing cybersecurity risks. The policy defines governance structure, risk management approach, and performance monitoring mechanisms, ensuring continuous alignment with regulatory and business requirements. Records within the document evidenced periodic reviews and updates based on evolving threats and organizational risk posture. Overall, the evidence indicates that the Bank maintains a well-defined and regularly reviewed cybersecurity policy aligned with the GV.PO control objective. **Documentary Evidences Reviewed:** • **Cyber Security Policy V2.5 FY 25-26.pdf**
4	**GV.OV: Oversight:** Results of organization-wide cybersecurity risk management activities, performance, and outcomes are used to inform, improve, and adjust the risk management strategy.	Based on discussions with the Canara Bank team, it was observed that the Bank did not have an automated tool or suitable dashboards in place for submitting and monitoring CCI compliance. Consequently, the Cyber Capability Index (CCI) assessment was performed	NA	Open	Medium	CIA	NA	The Bank has not implemented an automated Cyber Capability Index (CCI) assessment solution or integrated	The absence of an automated tool and integrated dashboards for Cyber Capability Index (CCI) assessment may lead to increased operational effort and a higher likelihood of human error in tracking	The Bank should plan and complete a formal Cyber Capability index (CCI) assessment covering all key cybersecurity domains (governance, identity & access, network security, incident	31-03-2026	All parameters related to CCI-as this is the initial assessment for the Canara Bank are being tracked and monitored periodically through manual process. However, the overall CCI score is currently being calculated manually.	Not Applicable	The assessor during the assessment interviewed the Canara Bank Personnel and reviewed the ISC Risk Assessment Report March 2025, the DP Secure Risk Register, and the Quarterly Report on Cyber Security Preparedness for June 2025 and noted that the Bank periodically reviews cybersecurity risks and performance against defined objectives. The results of these reviews, including simulation outcomes and control effectiveness, are used to refine and update the Bank's risk management strategy. However, it was observed that Canara Bank does not utilize an automated solution for conducting the Cyber Capability Index (CCI) assessment. The assessment has instead been carried out manually to determine the maturity of the bank's cybersecurity capabilities. **Documentary Evidences Reviewed:** • **ISC_Risk Assessment_March 2025.pdf (For ASBA, Citos & Kondor+)** • **Quarterly Report on Cyber Security Preparedness for June 2025.pdf** • **Dp secure risk register.xlsx**

Internal
Internal

Internal

		manually.						compliance dashboards due to the absence of a dedicated system and supporting workflows for automated CCI monitoring and reporting, resulting in reliance on manual processes.	assessing, and reporting, cybersecurity maturity. Manual execution can result in delays, reduced consistency and accuracy of compliance data, and limited real-time visibility into cybersecurity posture. This may further impede timely decision-making, weaken oversight across security domains, and potentially affect the Bank's ability to demonstrate continuous and structured cybersecurity capability improvement to regulatory bodies.	response, and recovery) and document outcomes for management review and remediation planning.		The process for automation CCI computation is presently underway.		
5	**GV.RM: Risk Management:** The RE's priorities, constraints, risk tolerance and risk appetite statements, assumptions and constraints are established, communicated, and used to support operational risk decisions.	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	No	The assessor during the assessment interviewed the Canara Bank personnel, reviewed documents, and examined evidences supporting the Bank's cybersecurity risk management framework. It was confirmed that the Bank has established and documented its risk priorities, constraints, tolerance, and appetite statements, which are approved by management and communicated across relevant functions. The following evidences were reviewed to assess compliance with SEBI's requirement GV.RM: Risk Management, and to validate that these elements are effectively used to support operational risk decisions.

Internal
Internal
Internal

Internal

														Documentary Evidences Reviewed: • **Cyber Security Policy_V2.5_FY 25–26.pdf** • **ISC_Risk Assessment_March 2025.pdf** • **Cyber Crisis Management Plan_V2.5_FY 25–26.pdf**
6	**GV.SC: Cybersecurity Supply Chain Risk Management:** The RE's priorities, constraints, risk tolerance, and assumptions are established and used to support decisions associated with managing supply chain risks. The RE has established and implemented the processes to identify, assess and manage supply chain risks.	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	No	The assessor during the assessment interviewed the Canara Bank personnel and reviewed documents, and examined evidences supporting the Bank's processes for identifying, assessing, and managing cybersecurity risks across its supply chain and noted that the Bank has defined and documented its priorities, risk tolerance, and assumptions, which are used to guide decision-making in the management of third-party and vendor-related risks. The review also verified that the Bank has implemented governance mechanisms, such as vendor due diligence, security assessments, and Software Bill of Materials (SBOM) maintenance for ASBA, DPsecure, CITOS and Kondor Plus has been reviewed, to ensure continuous monitoring of supply chain risks. The following evidences were reviewed to assess compliance with SEBI's requirement GV.SC: Cybersecurity Supply Chain Risk Management. **Documentary Evidences Reviewed:** 1. **IT Services Outsourcing Policy_2025–26.pdf** 2. **ASBA Vendor Agreement.pdf** 3. **DP Secure_Agreement.pdf** 4. **K+MASTER AGREEMENT.pdf** 5. **CITOS_SLA.pdf** 6. **Cybersecurity Policy_V.25_FY 2025–26.pdf** 7. **Man Power Tool_CS Wing-CSGITRMS_FINAL.xlsx** 8. **DP Secure_SBOM.pdf** 9. **ASBA Excellex EIPO_SBOM.docx** 10. **Canara Bank_Tata Consultancy Services_Vendor Risk Assessment Report_V1.1.pdf** 11. **Canara Bank_Canbank Computer Services Ltd (CCSL)_Vendor Risk Assessment Report_V1.1.pdf** 12. **Canara Bank_EXCELLEX Technologies_Vendor Risk Assessment Report_V1.1.pdf** 13. **Canara Bank_Finastra_Vendor Risk Assessment Final Report_V1.1.pdf** 14. **Canara Bank_Oracle_Vendor Risk Assessment Final Report_V1.1.pdf – 2 High Vulnerabilities Reported** 15. **D-DRILL_Aug 2025R.pdf** 16. **BCMS Framework_2025–26.pdf** 17. **SBOM for CITOS and Kondor reviewed**
7	**ID.AM: Asset Management:** The data, personnel, devices, systems, and facilities that enable the RE to achieve its business purposes are identified and managed consistently in accordance with their relative importance to organizational objectives and the RE's risk strategy	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	No	The assessor during the assessment interviewed the Canara Bank personnel, reviewed asset inventories, and examined evidences supporting the Bank's asset management process and noted that critical data, systems, and infrastructure are identified, documented, and maintained in alignment with the Bank's business and risk management framework. Additionally, IT assets are managed through the centralized IT-BRM application, and the asset inventory extract was obtained from IT-BRM.

Internal

Internal

Internal

														Documentary Evidences Reviewed: • SEBI-Assets.xlsx • BCMS Framework – Domestic 2025–26.pdf • Information Security Policy_V7.5_FY 25–26.pdf • ISG_V7.5_FY 25–26.pdf • cert in mail.docx • ASBA Secure – Done • DP Secure – DP Secure Server List • Artifacts_DP Secure_ • SSL List_Integrated Treasury Vertical • Application Details_Integrated Treasury Vertical • ASBA Network Diagram (Version History Not Updated) • DP Secure Architecture Diagram • Screenshot_DP Secure_EOL • SEBI CSCRF Audit Hardening Final evidences
8	**ID.RA: Risk Assessment:** The cybersecurity risk to the organization, assets, and individuals is assessed and understood by the RE.	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	No	The assessor during the assessment interviewed Canara Bank personnel, reviewed documents, and examined evidences supporting the Bank's cybersecurity risk assessment process and noted that the Bank periodically identifies, analyzes, and evaluates cybersecurity risks to its assets, systems, and personnel through formal assessments and ongoing monitoring. Risk assessment results are reviewed by management and integrated into the overall risk management framework. Documentary Evidences Reviewed: • ISC_Risk Assessment_March 2025.pdf • Monthly Note_August 2025_Alerts.pdf • CERT-IN FEB 2025.xlsx • cert in mail.docx • CYBERSECURITY POLICY V.25 - FY2025-26.pdf. • CERT-IN FEB 2025.xlsx • IT Risk Assessment Note-RMCB-March 2025.pdf • dp secure risk register.xlsx
9	**PR.AA: Identity Management, Authentication, and Access Control:** Access to physical and logical assets and associated facilities is limited to authorized users, processes and devices, and is managed commensurate with the assessed risk of unauthorized access.	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	No	The assessor during the assessment interviewed Canara Bank personnel, reviewed documents, and examined evidences supporting the Bank's cybersecurity risk assessment process and noted that the access to both physical and logical assets is restricted to authorized users and managed through defined authentication and authorization mechanisms. Multi-Factor Authentication (MFA), privileged access controls, and network segregation are implemented in accordance with the Bank's Information Security Policy. Documentary Evidences Reviewed: • Binding Processes for DP Secure and ASBA – Done • Monthly Performance Note_July 2025.pdf • PIM_MFA.doc • Information Security Policies_V7.5_FY 25–26.pdf • ASBA secure done • DP secure -DP secure server list

Internal

Internal

Internal

													• Network Architecture Diagram • ASBA Network Diagram (Version History Not Updated) • DP Secure Architecture Diagram • SEBI CSCRF Audit Hardening Final evidences
10	PR.AT: Awareness and Training: The RE's personnel and partners are provided cybersecurity awareness education, and are trained to perform their cybersecurity related duties and responsibilities consistent with related policies, procedures, and agreements.	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	No	The assessor during the assessment interviewed Canara Bank Personnel and reviewed the Cyber Security Awareness Communication (IT-Tech Vertical) email and noted that the Bank maintains a structured training calendar covering cybersecurity, cyber resilience, and system hygiene awareness programs. The Consolidated List of Half-Yearly Cyber Security Awareness – IT Staff (September 2025) evidenced employee participation and completion of training sessions. Training materials available on the Canarites Learning Portal include updated video modules and documents addressing emerging threats, with post-training assessments ensuring knowledge retention. The assessor also reviewed CISO Appointment Letters and Personnel Acknowledgment Records confirming understanding of cybersecurity roles and responsibilities across staff and senior management. Documentary Evidences Reviewed: • MAIL COMM FOR CYBER SECURITY AWARENESS SESSION (IT-TECH VERTICAL) (1).pdf • Consolidated List of Haly yearly Cyber security Awareness IT staff September 2025 (1) (1).pdf • Cyber Security Awarness Screenshots.docx • CISO Appoinment Letter.pdf, CISO of the Bank.pdf • personnel acknowledgement.docx
11	PR.DS: Data Security: Information and records (data) are managed consistent with the organization's risk strategy to protect the Confidentiality, Integrity, and Availability of information.	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	No	The assessor during the assessment interviewed the Canara Bank personnel, reviewed documents, and examined evidences supporting the Bank's data security management framework and noted that information and records are managed in alignment with the Bank's risk strategy to ensure confidentiality, integrity, and availability. Data Loss Prevention (DLP) controls, SSL configurations, and capacity management mechanisms are in place and the integrity verifications are monitored through SOC. It was also verified that data is stored within India, across facilities in Bangalore, Mumbai, and Hyderabad, in compliance with data localization requirements. Documentary Evidences Reviewed: • Information Security Policy_V7.5_FY 25-26.pdf • BCMS Framework_2025-26.pdf • Credit Risk Management – Data Management Policy_2025-26.pdf • Forcepoint DLP.docx • ISG_V7.5_FY 25-26.pdf • Artifacts_DP Secure_ • SSL List_Integrated Treasury Vertical • Application Details_Integrated Treasury Vertical • Vendor Secure Eyes_Audit Report (Dated 14 April 2024) • Canara Bank_Data Localisation_Compliance Report_V1.2_Updated_22-Apr-2024.pdf

Internal
Internal

Internal

														• June_2025_Capacity Management Note.pdf • Policy for Server Threshold Settings.pdf • Network Architecture Diagram • SOC Monthly Status Report_July 2025.pdf (Includes Alert Name, Count, Severity, Root Cause, and Action Taken) • SOC SEBI CSCRF Artefacts.pdf
12	**PR. IP: Information Protection Processes and Procedures:** Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	No	The assessor during the assessment interviewed the Canara Bank personnel, reviewed documents, and examined evidences supporting the Bank's information protection policies, processes, and procedures. It was confirmed that the Bank maintains and implements defined security policies covering roles, responsibilities, and management commitment towards protecting information systems and assets. The review also verified implementation through VAPT reports, patch compliance records, source code audits, and incident simulation exercises. However, it was observed that no Web Application Penetration Testing (WAPT) has been performed for the DP Secure application. Upon further discussion with Canara Bank personnel, it was noted that the Bank plans to decommission (discard) the DP Secure application by the end of November 2025. Documentary Evidences Reviewed: • ISG_V7.5_FY 25–26.pdf • ASBA VAPT 2nd Report.pdf • BCMS Framework_2025–26.pdf • Cyber Crisis Management Plan_V2.5_FY 25–26.pdf • BCMS Framework – Domestic_2025–26.pdf • ISO Certificate.pdf (Dated 2 May 2025) • R DRILL Report_Aug 26, 2025.pdf • Win OS Patch Compliance Report_DP Secure_Aug 2025.pdf • RHEL OS Patch Compliance Report_DP Secure_Aug 2025.pdf • OS Patch Compliance Report_ASBA_Aug 2025.pdf • ASBA Source Code Audit.pdf • DP Secure Source Code Audit.pdf (Dated 15 Mar 2025) • VAPT Reports by AKS dated 29th October 2024 for CITOS and Kondor+ • Canara Bank_ASBA_Web Application_Pentest_Report_v1.1_07 May 2025.pdf • Binding Processes for DP Secure and ASBA – Done • Monthly Performance Note_July 2025.pdf • Web Application Firewall Simulation Evidence • ASBA Server VAPT Closed Report (Load Balancer IPs are excluded) • VA_CMSC Mumbai_16 Jan 2025 • Web Application Security Audit Report_CITOS_30 Aug 2025 • Web Application Security Audit Report_ASBA SAS Application_31 Aug 2025.pdf • Web Application Security Audit Report_FOC_30 Aug 2025 • Cyber Security Audit Report_Dated 27 Jun 2025

Internal

Internal

Internal

														• **June_2025_Capacity Management Note** • **Policy for Server Threshold Settings** • **Hardening Evidence Dated 26 Mar 2025** • **SEBI CSCRF Audit Hardening Final evidences**
13	**PR.MA: Maintenance:** Maintenance and repairs of organizational control and information system components are performed consistent with policies and procedures.	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	No	The assessor during the assessment interviewed the Canara Bank personnel, reviewed documents, and examined evidences supporting the Bank's maintenance and patch management practices. It was confirmed that maintenance activities, including operating system patching, source code reviews, and application updates, are performed in line with approved policies and procedures. The Bank ensures regular review and timely remediation of identified vulnerabilities across key systems and applications. **Documentary Evidences Reviewed:** • **Information Security Guidelines V7.5 FY 25-26.pdf** • **Information Security Policy V7.5 FY 25-26.pdf** • **Win OS Patch Compliance Report-DPSECURE-Aug2025.pdf** • **RHEL OS Patch Compliance Report-DPSECURE-Aug2025.pdf** • **OS Patch Compliance Report_ASBA-Aug2025.pdf** • **Kondor – DCKPLUSAP01 ORACLE SOLARIS 11.4** • **Citos – ORACLE SOLARIS 11.4** • **PIM MFA.doc** • **ASBA Source code audit.pdf September 11, 2025** • **dp secure source code audit.pdf March 15 ,2025** • **SEBI CSCRF Audit Hardening Final evidences**
14	**DE.CM: Security Continuous Monitoring:** The REs' information systems and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	No	The assessor during the assessment interviewed the Canara Bank personnel, reviewed documents, and examined evidences supporting the Bank's continuous security monitoring framework. It was confirmed that the Bank's information systems and assets are monitored through a centralized SIEM solution integrated with the NGSOC to detect, analyse, and respond to cybersecurity events. Periodic monitoring reports, VAPT results, and system audit records demonstrate ongoing verification of the effectiveness of protective measures and incident response capabilities. However, it was observed that no Web Application Penetration Testing (WAPT) has been performed for the DP Secure application. Upon further discussion with Canara Bank personnel, it was noted that the Bank plans to decommission (discard) the DP Secure application by the end of November 2025. **Documentary Evidences Reviewed:** • **SOP for SIEM.pdf** • **NGSOC PO.pdf (Sample Screenshot from NetWitness SIEM)** • **SOC Monthly Status Report_July 2025.pdf (Includes Alert Name, Count, Severity, Root Cause, and Action Taken)** • **SOC SEBI CSCRF Artefacts.pdf** • **VAPT Reports_Dated March 2025**

Internal
Internal

Internal

														• INVA Reports_Dated April 2025 • June_2025_Capacity Management Note.pdf • Policy for Server Threshold Settings.pdf • Web Application Security Audit Report_CITOS_30 August 2025.pdf • Web Application Security Audit Report_ASBA SAS Application_31 August 2025.pdf • VAPT Reports by AKS dated 29th October 2024 for CITOS and Kondor+ • Web Application Security Audit Report_FOC_30 August 2025.pdf • Cyber Security Audit Report_Dated 27 June 2025.pdf • Canara Bank_ASBA_Web Application_Pentest_Report_v1.1_07 May 2025.pdf • ASBA Server VAPT Closed Report.pdf (Load Balancer IPs are excluded) • VA_CMSC Mumbai_16 January 2025.pdf • System Audit Report (Auditor Report).pdf
15	**DE.DP: Detection Process** Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	No	The assessor during the assessment interviewed the Canara Bank Personnel and reviewed the Cyber Crisis Management Plan V2.5 FY 25–26 and the SOP for SIEM and noted that the Bank has established defined roles, responsibilities, and procedures for detecting and responding to anomalous events. The SOC structure, detection playbooks, and notification procedures ensure effective monitoring and escalation in line with regulatory requirements. The Threat Hunting Reports for May–July 2025 evidenced proactive detection activities, and Red Teaming exercises are being conducted, with reports pending submission. Overall, the evidence indicates that the Bank maintains a structured and effective detection process aligned with the DE.DP control objective. **Documentary Evidences Reviewed:** • Cyber Crisis Management Plan V2.5 FY 25-26.pdf • SOP for SIEM.pdf • Web Gateway Simulations - Report v1.0.xlsx • RED TEAM JULY.pdf • Threat hunting Activity_May 2025.pdf • Threat Hunting June_2025.pdf • Threat Hunting Activity_July 2025.pdf
16	**RS.MA: Incident Management:** Incident response plans and procedures are executed and maintained in order to ensure response to detected/ known cybersecurity incidents.	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	No	The assessor during the assessment interviewed the Canara Bank Personnel and reviewed the Cyber Crisis Management Plan V2.5 FY 25–26 and noted that the Bank has established incident response procedures covering detection, containment, eradication, and recovery activities to ensure effective management of cybersecurity incidents. The plan defines roles, responsibilities, escalation matrices, and coordination mechanisms with internal and external stakeholders. The Incident Training Report – July 2025 evidenced that personnel responsible for incident response have undergone relevant training to maintain operational readiness. The BCMS Framework 2025–26 and Business Continuity Plan – Domestic 2025–26 further demonstrated integration between incident response and business continuity processes. The Quarterly Report on Cyber Security Preparedness for June 2025 confirmed that no cybersecurity incidents occurred during the assessment period.

Internal

Internal

														Documentary Evidences Reviewed: • **Cyber Crisis Management Plan V2.5 FY 25-26.pdf** • **Quarterly Report on Cyber Security Preparedness for June 2025.pdf** • **Incident Training Report July 2025** • **BCMS Framework- Domestic 2025-26 – Business Continuity Plan.pdf** • **BCMS Framework_ 2025-26.pdf** • **Certin mail august 23,2024**
17	**RS.CO: Incident Response Reporting and Communication:** Response activities are coordinated with internal and external stakeholders (e.g. external support from CERT-In, law enforcement agencies, etc.). Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	No	The assessor during the assessment interviewed the Canara Bank Personnel and reviewed the Cyber Crisis Management Plan and noted that response activities are coordinated with relevant internal and external stakeholders, including CERT-In and law enforcement agencies, as applicable, the assessor further noted that Canara has defined escalation and notification processes to ensure timely coordination and information sharing during security incidents. Additionally, evidence reviewed confirmed that voluntary information sharing with external stakeholders occurs, supporting broader cybersecurity situational awareness and alignment with the RS.CO objective. **Documentary Evidences Reviewed:** • **Cyber Crisis Management Plan V2.5 FY 25-26.pdf**
18	**RS.AN: Incident Analysis:** Incident analysis is conducted to ensure effective response and support recovery activities.	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	No	The assessor during the assessment interviewed the Canara Bank Personnel and reviewed the Cyber Crisis Management Plan V2.5 FY 25–26 and noted that processes are defined for conducting incident analysis to support effective response and recovery, including procedures for detection, categorization, root cause analysis, and post-incident review. The Quarterly Report on Cyber Security Preparedness for June 2025 confirmed that no cybersecurity incidents occurred during the assessment period. Overall, the evidence indicates that the Bank has a defined framework for incident analysis aligned with the RS.AN control objective. **Documentary Evidences Reviewed:** • **Cyber Crisis Management Plan V2.5 FY 25-26.pdf** • **Quarterly Report on Cyber Security Preparedness – June 2025.pdf**
19	**RS.IM: Improvements:** RE's response activities are improved by incorporating lessons learned from current and previous detection/ response activities.	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	No	The assessor during the assessment interviewed the Canara Bank Personnel and reviewed the Cyber Crisis Management Plan V2.5 FY 25–26 and confirmed that the Bank has defined procedures to document lessons learned and implement improvements in its incident response process. Updated policies and plans are communicated to stakeholders through the Cannet Portal, ensuring awareness of any changes. As per the Quarterly Report on Cyber Security Preparedness for June 2025, no incidents occurred during the assessment period. Overall, the evidence indicates that the Bank maintains a structured process for continuous improvement of its incident response framework, aligned with the RS.IM control objective. **Documentary Evidences Reviewed:** • **Cyber Crisis Management Plan V2.5 FY 25-26.pdf**

Internal

Internal

Internal

														• **Quarterly Report on Cyber Security Preparedness – June 2025.pdf** • **Internal Communication Portal.docx**
20	**RC.RP: Incident Recovery Plan Execution:** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity incidents.	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	No	The assessor reviewed the BCMS Framework 2025–26 and the Business Continuity Plan and noted that the Bank has defined recovery plans with cyber-scenario classifications, RTOs, and RPOs for critical systems in line with SEBI guidelines. The plans include backup and recovery procedures to ensure timely restoration of systems and data. The DR Drill Report dated August 26, 2025 evidenced that regular recovery drills are conducted to validate recovery readiness. Overall, the evidence indicates that the Bank maintains a robust and tested recovery framework aligned with the RC.RP control objective. **Documentary Evidences Reviewed:** • **Business Continuity Plan.pdf** • **BCMS Framework_ 2025-26.pdf** • **R DRILL Report_ Aug 26, 2025.pdf**
21	**RC.CO: Incident Recovery Communication:** Restoration activities are coordinated with internal and external stakeholders.	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	No	The assessor during the assessment interviewed the Canara Bank Personnel and reviewed the Cyber Crisis Management Plan V2.5 FY 25–26 and confirmed that the Bank has defined a Public Relations Management Strategy and Communication Plan to ensure effective coordination with internal and external stakeholders during recovery activities. The plans outline communication roles, escalation protocols, and timelines to maintain transparency and manage reputation during incidents. As per the Quarterly Report on Cyber Security Preparedness for June 2025, no incidents occurred during the assessment period, hence there were no communication records Overall, the evidence indicates that the Bank has a structured framework for coordinated recovery communication, aligned with the RC.CO control objective. **Documentary Evidences Reviewed:** • **Cyber Crisis Management Plan V2.5 FY 25-26.pdf** • **Quarterly Report on Cyber Security Preparedness – June 2025.pdf**
22	**RC.IM: Improvements:** Recovery planning and processes are improved by incorporating lessons learned from execution of recovery plans and processes.	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	No	The assessor during the assessment interviewed the Canara Bank Personnel and reviewed the BCMS Framework 2025–26 and the Business Continuity Plan – Domestic 2025–26 and confirmed that the Bank has defined processes to enhance recovery planning through lessons learned from recovery exercises and testing. The DR Drill Report dated August 26, 2025 evidenced that periodic drills are conducted to assess recovery effectiveness and identify improvement areas. Overall, the evidence indicates that the Bank follows a structured approach for continuous improvement of recovery processes, aligned with the RC.IM control objective. **Documentary Evidences Reviewed:** • **Business Continuity Plan.pdf** • **BCMS Framework_ 2025-26.pdf** • **DR DRILL Report_ Aug 26, 2025.pdf**

Internal

Internal

Internal

23	**EV.ST: Strategies:** A major component of cyber resilience is the ability to adapt and improve the security posture to stay ahead of threats.	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	No	The assessor during the assessment interviewed the Canara Bank personnel and reviewed the ISC Risk Assessment Report – March 2025 and confirmed that the Bank regularly identifies vulnerabilities and weaknesses to strengthen its cybersecurity posture. The Threat Hunting Report – July 2025 evidenced proactive threat intelligence and monitoring activities aimed at anticipating emerging risks. The Patch Compliance Reports for ASBA and DP Secure (Windows and RHEL) demonstrated timely remediation and system diversity to minimize exposure. The Cyber Security Framework Compliance Audit Reports for FY 2023–24 and FY 2024–25, along with the Tabletop Exercise Report September 2025, confirmed periodic reviews and resilience testing aligned with regulatory benchmarks. The Quarterly Report on Cyber Security Preparedness for June 2025 noted that no cybersecurity incidents occurred during the assessment period. Additionally, the assessor reviewed the CITOS and Kondor+ architecture diagrams from the SOP, reviewed on 4th August 2025, which evidenced defined system architecture and control segregation. **Documentary Evidences Reviewed:** • **ISC_Risk Assessment_March 2025.pdf** • **Threat Hunting Activity_July 2025.pdf** • **Citos and K+ architecture diagram reviewed from SOP, reviewed on 4th August 2025.** • **Win OS Patch Compliance Report-DPSECURE-Aug2025.pdf** • **RHEL OS Patch Compliance Report-DPSECURE-Aug2025.pdf** • **OS Patch Compliance Report_ASBA-Aug2025.pdf** • **Quarterly Report on Cyber Security Preparedness for June 2025.pdf** • **Canara_Bank_RBI_CSF_Compliance_Audit Report_2023-2024.pdf** • **Canara Bank-Cyber Security Framework-Compliance Audit-FY 2024-2025.pdf** • **Table Top Exercise- Table Top_sept 2025.pdf** • **Network architecture diagram** • **ASBA network diagram (Version history not updated)** • **DP secure architecture diagram** • **Kondor – DCKPLUSAP01 ORACLE SOLARIS 11.4** • **Citos – ORACLE SOLARIS 11.4**

Internal

Internal

3 Conclusion

ControlCase has determined that **CANARA BANK** is Compliant with the SEBI Circular **SEBI/HO/ ITD-1/ITD_CSC_EXT/P/CIR/2024/113 dated 20th August 2024 and SEBI/HO/ ITD-1/ITD_CSC_EXT/P/CIR/2025/119 dated, 28th August 2025**

Internal

Internal

Internal

Internal

Alcumus ISOQAR

Certificate of Registration

This is to certify that the Management System of:

Canara Bank
Information Technology Wing: Head Office (Annex), Naveen Complex, 14 M G Road, Bengaluru 560001, Karnataka, India

has been approved by Alcumus ISOQAR and is compliant with the requirements of:

ISO 27001:2022

SCOPE OF REGISTRATION

Internal

The Information Security Management System applies to the management of all Information Assets within the IT Infrastructure that support Canara Bank's Business Operations. This includes Servers, Devices, and Networks operating from its Datacentres, Near Datacentres, and Disaster Recovery Sites, covering functional areas such as the Information Technology Wing, Digital Banking Services Wing, Technology Operations Wing, Strategy and Data Analytics Wing, Centralized Procurement and Vendor Management Wing, Operations Wing (including the Reconciliation Vertical and Transaction Monitoring Vertical – EFRM Section), Cyber Security Wing, Human Resources Wing, Integrated Treasury Wing (SWIFT) and, Credit & Prepaid Cards Wing. This is in accordance with Statement of Applicability version 2.2 dated 14-2-2025

SIGNED

Jim Anderson, Chief Executive Officer
(on behalf of Alcumus ISOQAR)

CERTIFICATE NUMBER: **22100-ISMS-001**

Initial Registration Date:	12 April 2014
Previous Expiry Date:	11 April 2023
Recertification Audit Date:	06 – 08 April 2023
Re-Issue Date:	02 May 2025
Current Expiry Date:	11 April 2026

This certificate will remain current subject to the company maintaining its system to the required standard. This will be monitored regularly by Alcumus ISOQAR. Further clarification regarding the scope of this certificate and the applicability of the relevant standards' requirement may be obtained by consulting Alcumus ISOQAR.

Alcumus ISOQAR Limited, Cobra Court, 1 Blackmore Road, Stretford, Manchester M32 0QY
T: 0161 865 3699 E: isoqarenquires@alcumus.com W: isoqar.com
This certificate is the property of Alcumus ISOQAR and be returned of request.

Internal
Internal

Internal

Alcumus ISOQAR

Certificate Annex

Canara Bank

Annex 1 of 6 to Certificate number 22100-ISMS-001
Containing 3 locations including Head Office

12 April 2014

ISO 27001:2022

SCOPE OF REGISTRATION

The Information Security Management System applies to the management of all Information Assets within the IT Infrastructure that support Canara Bank's Business Operations. This includes Servers, Devices, and Networks operating from its Datacentres, Near Datacentres, and Disaster Recovery Sites, covering functional areas such as the Information Technology Wing, Digital Banking Services Wing, Technology Operations Wing, Strategy and Data Analytics Wing, Centralized Procurement and Vendor Management Wing, Operations Wing (including the Reconciliation Vertical and Transaction Monitoring Vertical – EFRM Section), Cyber Security Wing, Human Resources Wing, Integrated Treasury Wing (SWIFT) and, Credit & Prepaid Cards Wing. This is in accordance with Statement of Applicability version 2.2 dated 14-2-2025

Internal

SIGNED

Jim Anderson, Chief Executive Officer
(on behalf of Alcumus ISOQAR)

HEAD OFFICE

003 Information Technology Wing:
Head Office (Annex), Naveen Complex, 14 M G Road, Bengaluru 560001, Karnataka, India

OTHER LOCATIONS

004 Data Centre:
Canara Bank, ITI - Trimax Data Center, F-21, Gate no 5, ITI Complex, Doorvani Nagar, Bengaluru - 560 016

005 Near Data Centre:
Bangalore Canara Bank, ITI - Trimax Data Center, F-17, Gate no 5, ITI Complex, Doorvani Nagar, Bengaluru - 560 016, Karnataka, India

This certificate will remain current subject to the company maintaining its system to the required standard. This will be monitored regularly by Alcumus ISOQAR.
Further clarification regarding the scope of this certificate and the applicability of the relevant standards' requirement may be obtained by consulting Alcumus ISOQAR.

Alcumus ISOQAR Limited, Cobra Court, 1 Blackmore Road, Stretford, Manchester M32 0QY
T: 0161 865 3699 **E:** isoqarenquires@alcumus.com **W:** isoqar.com
This certificate is the property of Alcumus ISOQAR and be returned of request.

Internal
Internal

Internal

Alcumus ISOQAR

Certificate Annex

Canara Bank

Annex 2 of 6 to Certificate number 22100-ISMS-001
Containing 3 locations including Head Office

12 April 2014

ISO 27001:2022

SCOPE OF REGISTRATION

The Information Security Management System applies to the management of all Information Assets within the IT Infrastructure that support Canara Bank's Business Operations. This includes Servers, Devices, and Networks operating from its Datacentres, Near Datacentres, and Disaster Recovery Sites, covering functional areas such as the Information Technology Wing, Digital Banking Services Wing, Technology Operations Wing, Strategy and Data Analytics Wing, Centralized Procurement and Vendor Management Wing, Operations Wing (including the Reconciliation Vertical and Transaction Monitoring Vertical – EFRM Section), Cyber Security Wing, Human Resources Wing, Integrated Treasury Wing (SWIFT) and, Credit & Prepaid Cards Wing. This is in accordance with Statement of Applicability version 2.2 dated 14-2-2025

Internal

SIGNED

Jim Anderson, Chief Executive Officer
(on behalf of Alcumus ISOQAR)

HEAD OFFICE

003 Information Technology Wing:
Head Office (Annex), Naveen Complex, 14 M G Road, Bengaluru S60001

OTHER LOCATIONS

006 Disaster Recovery Site:
M/s.CtrlS Datacentres Limited. Plot No GEN 72/1/A, TTC Industrial Area, South Central Road, MIDC Industrial Area, Mahape, Thane, Navi Mumbai-400710, Maharashtra, India

008 Integrated Treasury Wing (SWIFT):
Head Office (Annex), Canara Bank Building, 5th-8th Floor, G Block, Bandra Kurla Complex, Bandra(E), Mumbai 400051, Maharashtra, India

This certificate will remain current subject to the company maintaining its system to the required standard. This will be monitored regularly by Alcumus ISOQAR. Further clarification regarding the scope of this certificate and the applicability of the relevant standards' requirement may be obtained by consulting Alcumus ISOQAR.

Alcumus ISOQAR Limited, Cobra Court, 1 Blackmore Road, Stretford, Manchester M32 0QY
T: 0161 865 3699 **E:** isoqarenquires@alcumus.com **W:** isoqar.com
This certificate is the property of Alcumus ISOQAR and be returned of request.

Internal
Internal

Internal

Alcumus ISOQAR

Certificate Annex

Canara Bank

Annex 3 of 6 to Certificate number 22100-ISMS-001
Containing 3 locations including Head Office

12 April 2014

ISO 27001:2022

SCOPE OF REGISTRATION

The Information Security Management System applies to the management of all Information Assets within the IT Infrastructure that support Canara Bank's Business Operations. This includes Servers, Devices, and Networks operating from its Datacentres, Near Datacentres, and Disaster Recovery Sites, covering functional areas such as the Information Technology Wing, Digital Banking Services Wing, Technology Operations Wing, Strategy and Data Analytics Wing, Centralized Procurement and Vendor Management Wing, Operations Wing (including the Reconciliation Vertical and Transaction Monitoring Vertical – EFRM Section), Cyber Security Wing, Human Resources Wing, Integrated Treasury Wing (SWIFT) and, Credit & Prepaid Cards Wing. This is in accordance with Statement of Applicability version 2.2 dated 14-2-2025

Internal

SIGNED

Jim Anderson, Chief Executive Officer
(on behalf of Alcumus ISOQAR)

HEAD OFFICE

003 Information Technology Wing:
Head Office (Annex), Naveen Complex, 14 M G Road, Bengaluru 560001

OTHER LOCATIONS

009 Cyber Security wing:
Head Office (Annex), 2nd Floor, NGV Commercial Complex, NGV, Koramangala, Bengaluru 560047, Karnataka, India

010 Digital Banking Services Wing:
Head Office (Annex), 86, Spencer Towers,3rd Floor, M G Road, Bengaluru 560001, Karnataka, India

This certificate will remain current subject to the company maintaining its system to the required standard. This will be monitored regularly by Alcumus ISOQAR. Further clarification regarding the scope of this certificate and the applicability of the relevant standards' requirement may be obtained by consulting Alcumus ISOQAR.

Alcumus ISOQAR Limited, Cobra Court, 1 Blackmore Road, Stretford, Manchester M32 0QY
T: 0161 865 3699 **E:** isoqarenquires@alcumus.com **W:** isoqar.com
This certificate is the property of Alcumus ISOQAR and be returned of request.

Internal
Internal

Internal

Alcumus ISOQAR

Certificate Annex

Canara Bank

Annex 4 of 6 to Certificate number 22100-ISMS-001
Containing 3 locations including Head Office

12 April 2014
ISO 27001:2022

SCOPE OF REGISTRATION

The Information Security Management System applies to the management of all Information Assets within the IT Infrastructure that support Canara Bank's Business Operations. This includes Servers, Devices, and Networks operating from its Datacentres, Near Datacentres, and Disaster Recovery Sites, covering functional areas such as the Information Technology Wing, Digital Banking Services Wing, Technology Operations Wing, Strategy and Data Analytics Wing, Centralized Procurement and Vendor Management Wing, Operations Wing (including the Reconciliation Vertical and Transaction Monitoring Vertical – EFRM Section), Cyber Security Wing, Human Resources Wing, Integrated Treasury Wing (SWIFT) and, Credit & Prepaid Cards Wing. This is in accordance with Statement of Applicability version 2.2 dated 14-2-2025

Internal

SIGNED

Jim Anderson, Chief Executive Officer
(on behalf of Alcumus ISOQAR)

HEAD OFFICE

003 Information Technology Wing:
Head Office (Annex), Naveen Complex, 14 M G Road, Bengaluru 560001

OTHER LOCATIONS

011 Technology Operations Wing:
Head Office (Annex), 6th Floor, Naveen Complex, 14 M G Road,
Bengaluru 560001, Karnataka, India

012 Strategy and Data Analytics Wing:
Head Office (Annex), Naveen Complex, 14 M G Road. Bengaluru 560001, Karnataka, India

This certificate will remain current subject to the company maintaining its system to the required standard. This will be monitored regularly by Alcumus ISOQAR. Further clarification regarding the scope of this certificate and the applicability of the relevant standards' requirement may be obtained by consulting Alcumus ISOQAR.

Alcumus ISOQAR Limited, Cobra Court, 1 Blackmore Road, Stretford, Manchester M32 0QY
T: 0161 865 3699 **E:** isoqarenquires@alcumus.com **W:** isoqar.com
This certificate is the property of Alcumus ISOQAR and be returned of request.

Internal
Internal

Internal

Alcumus ISOQAR

Certificate Annex

Canara Bank

Annex 5 of 6 to Certificate number 22100-ISMS-001
Containing 4 locations including Head Office

12 April 2014
ISO 27001:2022

SCOPE OF REGISTRATION

The Information Security Management System applies to the management of all Information Assets within the IT Infrastructure that support Canara Bank's Business Operations. This includes Servers, Devices, and Networks operating from its Datacentres, Near Datacentres, and Disaster Recovery Sites, covering functional areas such as the Information Technology Wing, Digital Banking Services Wing, Technology Operations Wing, Strategy and Data Analytics Wing, Centralized Procurement and Vendor Management Wing, Operations Wing (including the Reconciliation Vertical and Transaction Monitoring Vertical – EFRM Section), Cyber Security Wing, Human Resources Wing, Integrated Treasury Wing (SWIFT) and, Credit & Prepaid Cards Wing. This is in accordance with Statement of Applicability version 2.2 dated 14-2-2025

Internal

SIGNED

Jim Anderson, Chief Executive Officer
(on behalf of Alcumus ISOQAR)

HEAD OFFICE

003 Information Technology Wing:
Head Office (Annex), Naveen Complex, 14 M G Road, Bengaluru 560001

OTHER LOCATIONS

013 Centralized Procurement and Vendor Management wing:
Head Office (Annex). Naveen Complex, 14 M G Road, Bengaluru 560001, Karnataka, India

014 Operations Wing: a) Reconciliation Vertical at Bangalore:
Head Office (Annex) Naveen Complex, 14 M G Road, Bengaluru 560001, Karnataka, India

015 Operations Wing: b) Transaction Monitoring Vertical (EFRM Section) at Bangalore:
Head Office (Annex), Mezzanine floor, GandhiNagar, Bengaluru – 560009, Karnataka, India

This certificate will remain current subject to the company maintaining its system to the required standard. This will be monitored regularly by Alcumus ISOQAR.
Further clarification regarding the scope of this certificate and the applicability of the relevant standards' requirement may be obtained by consulting Alcumus ISOQAR.

Alcumus ISOQAR Limited, Cobra Court, 1 Blackmore Road, Stretford, Manchester M32 0QY
T: 0161 865 3699 **E:** isoqarenquires@alcumus.com **W:** isoqar.com
This certificate is the property of Alcumus ISOQAR and be returned of request.

Internal
Internal

Internal

Alcumus ISOQAR

Certificate Annex

Canara Bank

Annex 6 of 6 to Certificate number 22100-ISMS-001
Containing 3 locations including Head Office

12 April 2014
ISO 27001:2022

SCOPE OF REGISTRATION

The Information Security Management System applies to the management of all Information Assets within the IT Infrastructure that support Canara Bank's Business Operations. This includes Servers, Devices, and Networks operating from its Datacentres, Near Datacentres, and Disaster Recovery Sites, covering functional areas such as the Information Technology Wing, Digital Banking Services Wing, Technology Operations Wing, Strategy and Data Analytics Wing, Centralized Procurement and Vendor Management Wing, Operations Wing (including the Reconciliation Vertical and Transaction Monitoring Vertical – EFRM Section), Cyber Security Wing, Human Resources Wing, Integrated Treasury Wing (SWIFT) and, Credit & Prepaid Cards Wing. This is in accordance with Statement of Applicability version 2.2 dated 14-2-2025

Internal

SIGNED

Jim Anderson, Chief Executive Officer
(on behalf of Alcumus ISOQAR)

HEAD OFFICE

003 Information Technology Wing:
Head Office (Annex), Naveen Complex, 14 M G Road, Bengaluru 560001

OTHER LOCATIONS

016 Human Resources Wing:
Head Office-112, 3rd Floor, J C Road, Bengaluru 560002, Karnataka, India

017 Credit and Prepaid Cards Wing:
Head Office (Annex), Devanga Tower, 2nd Floor, 35, K G Road,
Bengaluru – 560009, Karnataka, India

This certificate will remain current subject to the company maintaining its system to the required standard. This will be monitored regularly by Alcumus ISOQAR.
Further clarification regarding the scope of this certificate and the applicability of the relevant standards' requirement may be obtained by consulting Alcumus ISOQAR.

Alcumus ISOQAR Limited, Cobra Court, 1 Blackmore Road, Stretford, Manchester M32 0QY
T: 0161 865 3699 **E:** isoqarenquires@alcumus.com **W:** isoqar.com
This certificate is the property of Alcumus ISOQAR and be returned of request.

Internal
Internal

Internal

केनरा बैंक Canara Bank

Cyber Security Wing, Head Office, Bangalore

Minutes of Meeting (MOM) of Information Security Committee held on 17.11.2025

Information Security Committee Chairman:

1. Shri. S K Majumdar, Executive Director

Information Security Committee Member Secretary & Convener:

1. Shri. A Ramesh babu, General Manager & CISO, CS Wing

Information Security Committee Members:

1. Shri. Purshottam Chand, Chief General Manager, Treasury Wing
2. Shri. Alok Kumar Agarwal, Chief General Manager, TS Wing
3. Shri. Dilli babu, General Manager, DBS Vertical, TS Wing
4. Shri. Amit Mittal, GCFO, General Manager, FM Wing
5. Shri. Adish Yadav, General Manager, RM Wing
6. Shri. Papanasam S, DPO, Deputy General Manager, S&DA Vertical, SR&GS Wing
7. Shri. Capt. Abhishek Srivastava, CSO, Divisional Manager, GA Wing

Participants Present:

1. Shri. S K L Das, General Manager, CPVM Vertical, TS Wing
2. Shri. T V Krishna Mohan, General Manager, TM Vertical, Operations Wing
3. Shri. Manoj Kumar, General Manager, Resources Vertical, SR&GS Wing
4. Shri. Rajesh R, General Manager, C&PC Vertical, TS Wing
5. Shri. Shreenath Joshi, General Manager, CLO, General Manager, CIBL, HR&PR Wing
6. Shri. Sudhakar Kotary, CP Vertical, Operations Wing
7. Smt. Muthulakshmi P, General Manager, CS Vertical, Operations Wing
8. Shri. Avinash Purohit, Deputy General Manager, IT Vertical, TS Wing
9. Shri. Vikas Mehta, Deputy General Manager, TO Vertical, TS Wing
10. Shri. Satyabrat Maharana, Asst. General Manager, CS Wing
11. Shri. Vadiraj S Kulkarni, Asst. General Manager, CS Wing
12. Shri. N Praveen Babu, Asst. General Manager, CS Wing
13. Shri. Keshav Kumar, Director, NCIIPC South

Internal

Shri. A Ramesh Babu, CISO, General Manager, CS Wing, Convener of the Committee welcomed the information Security Committee Chairman, members, and other participants and briefed about the agenda to be discussed in the meeting.

Internal

Internal

Agenda
Status on Compliance Audit of SEBI CSCRF

1. **Background:**

   On August 20, 2024, SEBI has formulated Cybersecurity and Cyber Resilience Framework (CSCRF) for its Regulated Entities (REs) to ensure adequate cyber resiliency.

2. **Discussion:**

- The CISO informed the committee that the SEBI CSCRF compliance audit was conducted by a Cert-In empanelled auditing firm and the final Cyber Audit Report (Annexure-A), SOC Efficacy (Annexure-N) Report has been submitted to the committee for the perusal.
- At present, as per our SEBI licenses, our Bank falls under the Qualified Regulated Entity (QRE) category, since our DP license (DP Secure package) is classified under QRE as per SEBI CSCRF. This pertains to the e-Syndicate Bank and as per the Board's directions, no DP operations are being carried out. Existing DP accounts (around 1500) related to ex-staff and staff are being closed or transferred as there are no operations.
- One pending point for SEBI CSCRF compliance audit is the implementation of the Automated Cyber Capability Index (CCI) tool. However, as per SEBI CSCRF, CCI report to be submitted annually and the submission not falls under this half year cycle.
- Our Bank currently does not have this automated Cyber Capability Index (CCI) tool and is in the process of exploring the same for implementation. A tentative timeline of 31.03.2026 has been set, this may be extended depending on industry readiness. Meanwhile, the CCI report has been prepared manually and presented to the auditor.
- Our subsidiary M/s CanBank Securities Limited (CBSL) holds NSDL license and our bank's DP license is with CDSL. Currently the process for obtaining the CDSL license by CBSL is currently underway. CBSL has submitted the application to CDSL, and the license approval is in progress.
- Once the CDSL license is obtained by CBSL, the DP accounts will be transferred to CBSL and the Bank will transfer the existing DP accounts to CDSL and will surrender its DP license. Consequently, the Bank will fall under the Small Size RE category, where complied with SEBI CSCRF compliance and Qualified RE requirements will no longer be applicable.
- The CISO further updated the committee that mandatory reports— Cyber Audit Report, SOC Efficacy Report and VAPT Report are required to be submitted to SEBI, NSE/BSE, and CDSL as per regulatory guidelines. Preparation of the detailed VAPT report is currently in progress and the final consolidated report will be submitted upon completion.
- All applicable reports will be submitted to SEBI and other respective agencies with the signature of the MD & CEO, and the submissions will be completed within this December 2025 month.

3. **Committee after deliberations:**

   The Committee deliberated and noted the contents of the above note.

A Ramesh Babu
General Manager & CISO

Internal

Internal

केनरा बैंक Canara Bank
सिंडिकेट Syndicate
Together We Can

Annexure-N : Functional Efficacy of SOC

Name of the Organisation: Canara Bank

Entity Type: Bank

Entity Category: Qualified Regulated Entity (Qualified RE)

Rationale for the Category: Canara Bank is registered under multiple licenses with SEBI and their classifications as per SEBI CSCRF are as Depository Participant (DP) - Qualified RE, Merchant Banker and Proprietary Stock Broker - small size RE and Bankers to an Issue (BTI) and Self-Certified Syndicate Banks (SCSBs).

As per SEBI CSCRF guidelines, where a Regulated Entity falls under multiple classifications, the compliance requirements applicable to the highest classification shall prevail. Since the Bank holds Depository Participant (DP) registration, which falls under the Qualified Regulated Entity (Qualified RE) classification, Canara Bank is accordingly classified under Qualified RE.

Period of Audit: 8th - 12th September 2025.

Authorised signatory declaration:

Internal

I hereby confirm that the report of functional efficacy of SOC has been verified by me and I shall take the responsibility and ownership of the report.

Signature:

Name of the signatory: K Satyanarayana Raju

Designation: MD-CEO

Company stamp:

CANARA BANK
MD & CEO's SCRT.
BENGALURU-2

Annexures:

Report of Functional efficacy of SOC.

Internal
Confidential

Internal

Table 01: Score calculation of SOC efficacy

Sr. No.	Domain	Weightage (%) [A]	Score [B]	Normalised Score [S]= (B x A)/100
1	Coverage of Assets	25	98.73	24.68
2	SOC Operations	25	88.28	22.07
3	Competency of SOC personnel	20	83.25	16.65
4	SOC Governance	15	55.62	8.34
5	SOC Enrichments	15	42.00	6.3
			Final Score (ΣS)	**78.04**

The detailed scoring system for the above-mentioned domains is given below:

a) Coverage of assets w.r.t SOC technologies: Integration of all assets with deployed SOC technologies is required in order to have holistic visibility over RE's IT environment. It shall help the RE in measuring the extent to which SOC technologies encompass the RE's entire asset base.

Internal

Table 02: IT Asset distribution of RE

Sr. No	System Types*	System type ID	Count
1	Network Devices (Switches, Load Balancers, Routers, Firewalls, etc.)	S1	484
2	Security Solutions (SOC and NOC technologies deployed)	S2	14
3	End-Points	S3	84731
4	Applications (Internal or External)	S4	537
5	Databases	S5	120
6	All Servers (such as AD, DHCP, DNS, Patch mgmt., NTP, IPT, Wi-Fi, Application server, **Database servers**, server-based security solutions, etc.)	S6	3805 (3685+120)

Internal

Internal

Table 03: Methodology to assess the level of asset integration with SOC Technologies

Sr.No.	SOC Technologies	Weightage (%) (W)	System ID applicable	Count of systems to be integrated (x) [to be identified from table [02]	Count of systems actually Integrated and covered (y)	Coverage Score Z=(y/x)	Weighted Score (Z*W)
1	PAM	10	S1	3805	3601	0.946	9.46
2	Anti-virus / Epp	10	S3, S6	88536 (84731+3805)	87960 (84359+3601)	0.993	9.93
3	EDR	10	S3	84731	84731	1	10
4	DLP	10		84731	84731	1	10
5	DAM	10	S5	120	119	0.991	9.91
6	WAF	10	S4	93	93	1	10
7	Email Gateway	10		1	1	1	10
8	Web Gateway	10		16	16	1	10
9	DDOS	10		2	2	1	10
10	SIEM	10	S1, S2, S4, S5, S6	4396 (484+14+ 93+3805)	4147 (439+14+ 93+3601)	0.943	9.43
	Technology-Asset -Coverage-percentage						98.73

Internal

Internal

Internal

b) **SOC Operations:** To determine the efficiency of the periodic activities carried out by SOC personnel for effective threat management and regular maintenance of SOC technologies.

Table 04: Methodology to assess the performance of SOC operations

Sr.No.	Metric	Value	Weightage (W) (%)	Weighted Score
1	**Log Injection into SIEM**		5	(A/B) *W **4.88**
	Log sources reporting to SIEM[A]	3601		
	Total No. of Log sources (from Table 01) [B]	3685		
2	**Latency in log injection**	(2Seconds)	5	IF C<5 then score= ((5-C)/5*W **4.96**
	Maximum log processing latency - latency between collection of the security event at log source and processing it in SIEM (in minutes) [C]			
3	**SOC technology version control**		5	(D/E) × W **2.14**
	No. of technologies running on version 'n-1' and 'n'[D]	3		
	Total no of technology deployed[E]	7		
4	**SOC technology vulnerability closure**		5	(F/G) ×W **0.23**
	No. of open advisories (issued by CERT-In/ CSIRT-Fin) and vulnerabilities on SOC technologies [F]	14		
	Total advisories (issued by CERT-In/ CSIRT-Fin) and vulnerabilities reported on SOC technologies [G]	292		
5	**SIEM Use cases**		5	(H/I) ×W **5.00**
	No. of SOC technologies for which use cases are configured [H]	14		
	Total no. of SOC technologies [I] (from Table 3)	14		
6	**Use cases that are not triggered**		5	((K-J)/K) ×W **2.23**
	Use-cases that are not triggered [J]	303		
	Total no. of use cases [K]	548		
7	**Playbooks Defined**		10	(L/M) ×W **10.00**
	No. of playbooks defined associated with use cases [L]	245		
	Total no. of use cases [M]	245		
8	**False Positives**		10	((O-N)/O) ×W **9.91**
	No. of false Positives(N)	16		
	Total no of alerts[O]	1814		

Internal
Confidential
Internal

Internal

केनरा बैंक Canara Bank
Together We Can

Sr.No.	Metric	Value	Weightage (W) (%)	Weighted Score
9	**False Negatives**		10	((Q-P)/Q) ×W **10.00**
	No. of false negatives [P]	0		
	Total no. of alerts [Q]	1814		
10	**Threat Intel (benchmarking against 60 minutes)**		5	IF R<60 then score = ((60-R) / 60) *W **4.16**
	Mean Time to process the Threat Intel feed received (minutes)[R]	10 minutes		
11	**Handling Critical Systems**			
	Critical Applications and assets' log injection in SIEM is being verified on a daily basis?	Yes=1 No=0 [S]	2	S×W **2.00**
	Critical Applications and assets' integration with Anti-virus/ EDR, DAM, etc. verified on a daily basis?	Yes=1 No=0 [T]	2	T×W **2.00**
	Use-cases/rules configured on SIEM for critical systems?	Yes=1 No=0 (U)	2	U×W **2.00**
	Privilege access to critical systems verified on a weekly basis?	Yes=1 No= 0 (V)	2	V×W **2.00**
	Configuration and data back-ups being taken periodically?	Yes=1 No=0 (X)	2	X×W **2.00**
12	**REs metrics**			
	MTTD (Mean Time to Detect): Incidents detected within defined TAT ***No of Incidents detected within defined TAT / Total No of Incidents**	11755/118839(w)	5	w*W **4.94**
	MTTR (Mean Time to Respond): Incidents responded within defined TAT ***No of Incidents resolved within defined TAT / Total No of Incidents**	11482/11883(Y)	5	Y*W **4.83**
	Phishing sites taken down: **No of phishing sites taken down / Total no of Phishing sites reported**	191/191(Z)	15	Z*W **15**
	Total			**88.28**

Internal

Confidential

Internal

Internal

C) Competency of deployed SOC personnel: To assess the skill level of security professionals deployed in SOC through a combination of appropriate industry level certifications and years of experience to ensure that SOC operations are carried out in smooth and effective manner.

Table 05: Methodology to assess the competency of deployed SOC personnel

Sr. No.	category of engineers	Minimum Certification requirement	Weightage of category [C] %	Years of experience (YoE)	weightage of sub category [w]	Count of engineers having minimum required certifications [x]	Actual sub category Score [z]=[x]*[w]	Category-wise score[A]= Sum[z] / Sum[x]	Weighted Score [B]=(A)*[c]
1	L1	CEH	35	2	0.25	0	0	1	35.00
2				3	0.50	0	0		
3				4	0.75	0	0		
4				5	1.00	6	6		
5	L2	CEH+OEM	25	6	0.33	6	1.98	0.33	8.25
6				7	0.66	0	0		
7				8	1.00	0	0		
8	L3	CEH+CISM	40	9	0.25	0	0	1	40.00
9				10	0.5	0	0		
10				11	0.75	0	0		
11				>=12	1.00	2	2		
							Final Score of Man Power		83.25

Internal
Confidential
Internal

Internal

d) SOC Governance: To determine the capability of strategic management and the level of oversight of SOC through factors such as finances, personnel training and the involvement of IT Committees for REs and their Board.

Table 06: Methodology to assess the governance of SOC

Sr. No	Metric	Value (A)	Weightage (W) (%)	Weighted Score
1	**Budget for SOC**		45	(2*B/A) ×W 45.00
	Budget spent on cybersecurity [A]	12.39		
	Budget Spent on SOC technology and governance (50% benchmarking) [B]	10.63		
2	**Training**			
	Percentage of budget spent for training out of total budget forecasted for training	[E] (1248400/20000000)	10	(E/100) ×W 0.62
3	Whether SOC review has been undertaken by *IT Committee for* Res	Yes=1, No=0 [F]	5	F×W 5
4	Whether recommendations of technology committee have been submitted to governing board of RE	Yes=1, No=0 [G]	5	G×W 5
		Total		55.62

Internal

Internal

E) SOC Enrichments and Enhancements: To determine the level of proactiveness of SOC in leveraging deployed technologies, automation of alert responses and deploying latest SOC technologies. This will help the SOC to evolve and ensure its preparedness in case of a future breach.

Table 07: Methodology to assess proactiveness of SOC

Sr.No.	Metric	Value(A)	Weightage(w) (%)	Weighted Score
1	**Dashboard and Analytics**			
1.1	Using Native technology dashboard	Yes=1, No=0	5	A×W 5
1.2	Custom developed dashboard	Yes=1, No=0	5	A×W 5
2	**Threat Hunting**			
2.1	Threat Hunting Exercise Carried out by:			
	Specialized Threat Hunting service provider	Yes=1, No=0	5	A×W 0
	Internal Team	Yes=1, No=0	3	A×W 3
2.2	Periodicity of the Exercise:			
	Quarterly	Yes=1, No=0	5	A×W 0
	Half-Yearly	Yes=1, No=0	3	A×W 3
2.3	**Hypotheses**			
	Total no of hypotheses [T]	0		
	No. of hypotheses based on the open vulnerabilities [X]	0	5	(X/T) ×W 0
	No. of Hypotheses based on IoCs [Y]	0	5	(Y/T) ×W 0
	No. of Hypotheses based on IoAs [Z]	0	5	(Z/T) ×W 0
3	**Automation**			
3.1	Threat intel integration with SIEM	Yes=1, No=0	5	A×W 5
3.2	No. of SOAR actions triggered [T]	0		
	Total no. of different SOAR actions created [S]	0	5	(T/S) ×W 0
4	**Technologies implemented**			
	Decoy	Yes=1, No=0	3	A×W 3

Internal

Internal

Sr.No.	Metric	Value(A)	Weightage(w) (%)	Weighted Score
	Sandboxing Solution	Yes=1, No=0	3	A×W 3
	UEBA	Yes=1, No=0	3	A×W 0
	Vulnerability Management Solution	Yes=1, No=0	3	A×W 3
	Encrypted Traffic Management	Yes=1, No=0	3	A×W 3
	DNS Security	Yes=1, No=0	3	A×W 3
	Intrusion prevention system	Yes=1, No=0	3	A×W 3
	Data classification solution	Yes=1, No=0	3	A×W 3
	Total		75	42

Internal

Confidential

Internal

Internal

केनरा बैंक Canara Bank

Cyber Security Wing, Head Office, Bangalore

Minutes of Meeting (MOM) of Information Security Committee held on 17.11.2025

Information Security Committee Chairman:

1. Shri. S K Majumdar, Executive Director

Information Security Committee Member Secretary & Convener:

1. Shri. A Ramesh babu, General Manager & CISO, CS Wing

Information Security Committee Members:

1. Shri. Purshottam Chand, Chief General Manager, Treasury Wing
2. Shri. Alok Kumar Agarwal, Chief General Manager, TS Wing
3. Shri. Dilli babu, General Manager, DBS Vertical, TS Wing
4. Shri. Amit Mittal, GCFO, General Manager, FM Wing
5. Shri. Adish Yadav, General Manager, RM Wing
6. Shri. Papanasam S, DPO, Deputy General Manager, S&DA Vertical, SR&GS Wing
7. Shri. Capt. Abhishek Srivastava, CSO, Divisional Manager, GA Wing

Participants Present:

1. Shri. S K L Das, General Manager, CPVM Vertical, TS Wing
2. Shri. T V Krishna Mohan, General Manager, TM Vertical, Operations Wing
3. Shri. Manoj Kumar, General Manager, Resources Vertical, SR&GS Wing
4. Shri. Rajesh R, General Manager, C&PC Vertical, TS Wing
5. Shri. Shreenath Joshi, General Manager, CLO, General Manager, CIBL, HR&PR Wing
6. Shri. Sudhakar Kotary, CP Vertical, Operations Wing
7. Smt. Muthulakshmi P, General Manager, CS Vertical, Operations Wing
8. Shri. Avinash Purohit, Deputy General Manager, IT Vertical, TS Wing
9. Shri. Vikas Mehta, Deputy General Manager, TO Vertical, TS Wing
10. Shri. Satyabrat Maharana, Asst. General Manager, CS Wing
11. Shri. Vadiraj S Kulkarni, Asst. General Manager, CS Wing
12. Shri. N Praveen Babu, Asst. General Manager, CS Wing
13. Shri. Keshav Kumar, Director, NCIIPC South

Shri. A Ramesh Babu, CISO, General Manager, CS Wing, Convener of the Committee welcomed the information Security Committee Chairman, members, and other participants and briefed about the agenda to be discussed in the meeting.

Internal

Internal

Agenda

Status on Compliance Audit of SEBI CSCRF

1. **Background:**

   On August 20, 2024, SEBI has formulated Cybersecurity and Cyber Resilience Framework (CSCRF) for its Regulated Entities (REs) to ensure adequate cyber resiliency.

2. **Discussion:**

- The CISO informed the committee that the SEBI CSCRF compliance audit was conducted by a Cert-In empanelled auditing firm and the final Cyber Audit Report (Annexure-A), SOC Efficacy (Annexure-N) Report has been submitted to the committee for the perusal.
- At present, as per our SEBI licenses, our Bank falls under the Qualified Regulated Entity (QRE) category, since our DP license (DP Secure package) is classified under QRE as per SEBI CSCRF. This pertains to the e-Syndicate Bank and as per the Board's directions, no DP operations are being carried out. Existing DP accounts (around 1500) related to ex-staff and staff are being closed or transferred as there are no operations.
- One pending point for SEBI CSCRF compliance audit is the implementation of the Automated Cyber Capability Index (CCI) tool. However, as per SEBI CSCRF, CCI report to be submitted annually and the submission not falls under this half year cycle.
- Our Bank currently does not have this automated Cyber Capability Index (CCI) tool and is in the process of exploring the same for implementation. A tentative timeline of 31.03.2026 has been set, this may be extended depending on industry readiness. Meanwhile, the CCI report has been prepared manually and presented to the auditor.
- Our subsidiary M/s CanBank Securities Limited (CBSL) holds NSDL license and our bank's DP license is with CDSL. Currently the process for obtaining the CDSL license by CBSL is currently underway. CBSL has submitted the application to CDSL, and the license approval is in progress.
- Once the CDSL license is obtained by CBSL, the DP accounts will be transferred to CBSL and the Bank will transfer the existing DP accounts to CDSL and will surrender its DP license. Consequently, the Bank will fall under the Small Size RE category, where complied with SEBI CSCRF compliance and Qualified RE requirements will no longer be applicable.
- The CISO further updated the committee that mandatory reports– Cyber Audit Report, SOC Efficacy Report and VAPT Report are required to be submitted to SEBI, NSE/BSE, and CDSL as per regulatory guidelines. Preparation of the detailed VAPT report is currently in progress and the final consolidated report will be submitted upon completion.
- All applicable reports will be submitted to SEBI and other respective agencies with the signature of the MD & CEO, and the submissions will be completed within this December 2025 month.

3. **Committee after deliberations:**

   The Committee deliberated and noted the contents of the above note.

A Ramesh Babu
General Manager & CISO

Internal