7

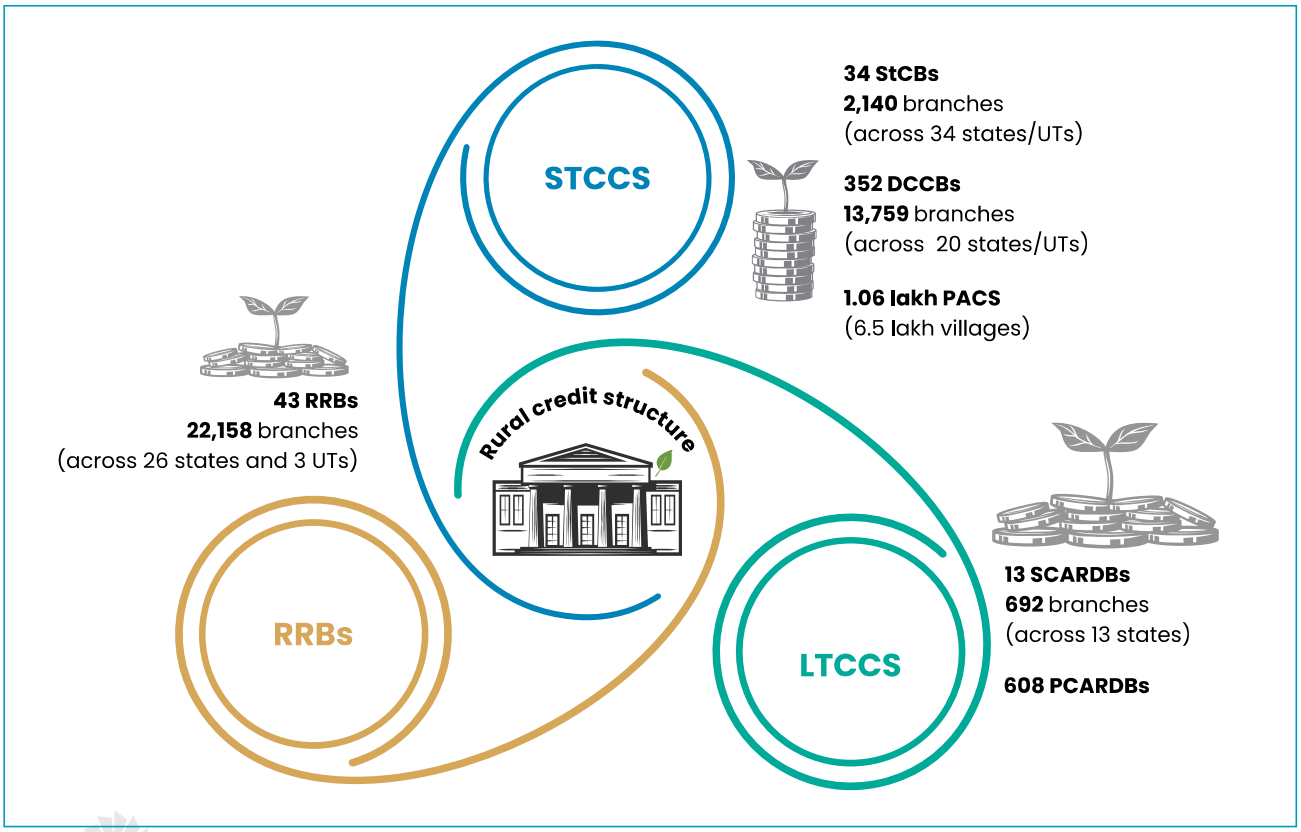
SUPERVISORY ROLE OF NABARD

Robust supervision of financial entities is essential for maintaining institutional integrity, safeguarding the interests of the depositors, and ensuring the smooth functioning of the financial ecosystem. As the apex institution in the field of agriculture and rural finance, NABARD plays a critical supervisory role over rural financial institutions (RFIs). This responsibility extends beyond routine oversight, reflecting a proactive commitment to the twin goods of deepening financial inclusion and fostering the development of RFIs. In addition, NABARD acts as a key advisor, supporting non-compliant banks in implementing corrective measures to restore financial stability and ensure long-term sustainability.

7.1 SUPERVISED ENTITIES OF NABARD

Regional rural banks (RRBs) and rural cooperative banks (RCBs) play a vital role in delivering financial services across rural India. As NABARD supervised entities (SEs), these institutions are subject to regular inspections by NABARD to ensure regulatory compliance and financial soundness. The RRBs and RCBs are regulated by the Reserve Bank of India (RBI) and supervised by NABARD under Section 35(6) of the Banking Regulation (BR) Act, 1949 and the BR Act, 1949 (As Applicable to Co-operative Societies), respectively. NABARD's supervisory activities encompass statutory inspections of state and district central cooperative banks (StCBs and DCCBs) and RRBs, as well as voluntary inspections of state cooperative agriculture and rural development banks (SCARDBs), apex weavers' societies, marketing federations, and other relevant entities, availing refinance from NABARD (Figures 7.1–7.2).

Figure 7.1: Rural institutional credit structure (as on 31 March 2025)



DCCB = District Central Cooperative Bank, LTCCS = Long-Term Cooperative Credit Structure, PACS = Primary Agricultural Credit Society, PCARDB = Primary Cooperative Agriculture and Rural Development Bank, RRB = Regional Rural Bank, SCARDB = State Cooperative Agriculture and Rural Development Bank, StCB = State Cooperative Bank, STCCS = Short-Term Cooperative Credit Structure, UT = Union Territory.

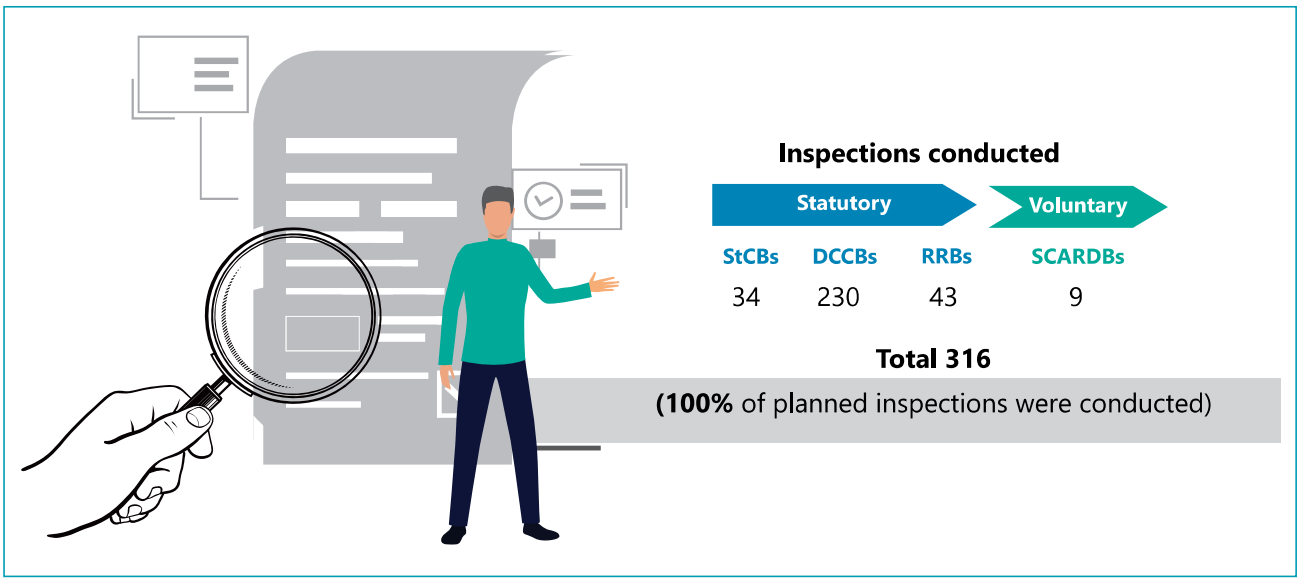
Notes:

1. Number of SEs as on 31 March 2025.
2. PACS and PCARDBs are not statutorily supervised entities.
3. Number of PACS as on 31 March 2023 (provisional data).
4. Of the 34 StCBs, 24 are Scheduled under the Second Schedule of the Reserve Bank of India Act, 1934.
5. The 352 DCCBs include Tamil Nadu Industrial Cooperative Bank, which is considered a DCCB only for the purposes of regulation and supervision. Malappuram DCCB has since been merged with Kerala StCB but the matter is subjudice.
6. There are variations in the cooperative credit structure across states. Not all STCCS have three tiers; some states have two-tier structure as well.
7. SCARDBs (13) categorised by nature of operations:
   a. Unitary (lending directly) (5): Gujarat, Jammu & Kashmir, Puducherry, Tripura, and Uttar Pradesh;
   b. Federal (lending through PCARDBs) (6): Haryana, Karnataka, Kerala, Punjab, Rajasthan, and Tamil Nadu; and
   c. Mixed (lending through both PCARDBs as well as directly) (2): Himachal Pradesh and West Bengal.
8. LTCCS
   a. The provisions of BR Act, 1949 are not applicable to these institutions.
   b. They do not have access to low-cost deposits.
   c. They depend heavily on borrowed funds for lending.
9. RRBs
   a. The RRBs are sponsored by 12 scheduled commercial banks.
   b. With effect from 1 May 2025, 43 RRBs were merged into 28 RRBs as part of the "One State, One RRB" policy.
   c. RRBs are operational in the UTs of Puducherry, Jammu &Kashmir, and Ladakh.
   d. 92% (provisional data) of the RRB branches are located in rural/semi-urban areas.
   e. There are no RRBs in the states of Goa and Sikkim.

Sources:

RBI (2024), Report on Trend and Progress in Banking in India, 2023–24, Reserve Bank of India, Mumbai. https://rbidocs.rbi.org.in/rdocs/Publications/PDFs/0RTP261220247FFF1F49DFC04C508F300904A90C7439.PDF.

Figure 7.2: Supervision by NABARD in FY2025



DCCB = District Central Cooperative Bank, RRB = Regional Rural Bank, SCARDB = State Cooperative Agriculture and Rural Development Bank, StCB = State Cooperative Bank.

Notes:

1. DCCBs include Tamil Nadu Industrial Cooperative Bank Ltd.
2. Supervision undertaken in FY2025 with respect to status of supervised entities as on 31 March 2024.

7.2 MAJOR DEVELOPMENTS IN THE SUPERVISORY ECOSYSTEM DURING FY2025

FY2025 witnessed notable advancements in NABARD's supervisory framework, reaffirming its commitment to reinforcing the resilience and stability of RFIs. Key developments included implementation of the Enhanced CAMELSC-based supervisory rating model with differential approach, alongside targeted initiatives to refine supervisory tools and strengthen the capabilities of supervised entities.[1]

7.2.1 Enhanced CAMELSC-based supervisory approach

The Enhanced CAMELSC-based supervisory rating model (E-CAMELSC) represented a significant evolution in NABARD's supervisory strategy. Rolled out comprehensively from 1 April 2023, this interim supervisory approach serves as a critical step towards a more robust risk-based supervision framework. The E-CAMELSC offers a structured methodology for evaluating the performance of SEs by integrating both qualitative and quantitative indicators. This holistic assessment is designed to establish the soundness of an institution's risk management systems, which are fundamental to institutional resilience. Based on their business size, 148 banks were inspected during FY2025 under the E-CAMELSC model. The principal developments during the year that further enhanced this approach are outlined below.

1. **Refinement in Enhanced CAMELSC Rating Model:** Recognising the evolving banking landscape, the E-CAMELSC supervisory rating model was significantly revised in April 2023. This update aligned the model's performance rating parameters with contemporary legal, regulatory, and supervisory guidelines, while also reflecting the increasing scale and complexity of banking operations. The revised model is structured to evaluate banks based on their financial position as on 31 March 2025.
2. **Review of guidelines on stress testing:** Given the climate of potential economic uncertainties, robust stress testing capabilities are imperative. During the year, a comprehensive review of the existing stress testing guidelines for banks was undertaken. This focused on enhancing the availability of data at the bank level and refining the stress testing template to facilitate the creation of realistic stress scenarios. These scenarios aim to reflect potential shifts in loan exposures within bank portfolios, thereby strengthening their capacity to withstand adverse conditions.
3. **Guidance notes on implementation of risk management systems in SEs:** Under the E-CAMELSC supervisory framework, the quality and effectiveness of risk management systems in SEs remain a priority. To reinforce this focus, guidance notes were issued to SEs, detailing the implementation of sound risk management frameworks across key areas such as operational risk management, credit risk management, business continuity planning, capital management, and, notably, liquidity risk management, with updated guidance on the latter issued in FY2025. This proactive support aims to enable SEs to establish and maintain effective risk management practices.
4. **Capacity building and training programmes:** Recognising the significance of skilled personnel in effective supervision, a series of targeted capacity building and training programmes were conducted during the year. These initiatives, grounded in both the theoretical and practical aspects of inspection under the E-CAMELSC model, were tailored for inspecting officers (IOs) and staff of supervised banks. This investment in human capital aimed to deepen understanding and promote effective application of the enhanced supervisory framework.

7.2.2 Digitalisation of inspection process through SuperSoft application

The SuperSoft application was launched on the occasion of NABARD's 41st Foundation Day on 12 July 2022. Since its inception, all statutory inspections have been conducted through this digital platform. During FY2025, statutory inspections of 307 banks—comprising 43 RRBs, 34 StCBs, and 230 DCCBs—were undertaken using the SuperSoft application.

As part of ongoing enhancements, the following modules were developed and operationalised in SuperSoft 2.0 during the year:

1. **Branch inspection module for RRBs:** This module enables inspection teams to conduct inspections of RRB branches and share their reports with the main team for reference.
2. **Inspection report scrutiny and grading module:** This functionality allows NABARD to scrutinise and grade inspection reports directly within the SuperSoft platform.
3. **Information technology/information security (IT/IS) examination module:** Designed for use by the Cyber Security and Information Technology Examination (CSITE) Cell of the Department of Supervision, NABARD at both the Head Office and the regional offices, this module facilitates the conduct of IT/IS examinations via the SuperSoft application.
4. **ENSURE 2.0 and SuperSoft API integration:** This integration ensures seamless data transfer between platforms, eliminating the need for manual uploads and simplifying the inspection workflow, while also improving data quality in SuperSoft.
5. **Management Information System (MIS) reports module:** A suite of nine MIS reports has been developed within SuperSoft to enable real-time monitoring of the inspection process—from planning and execution to dispatch and closure.
6. **Notifications module:** This module ensures timely email alerts for users, enabling prompt completion of tasks by minimising delays.
7. **Movement register module:** This feature tracks the movement of inspection reports and related documents at various levels, ensuring timely task execution and enhanced process accountability.

7.2.3 FATF *Mutual Evaluation Report*

The Financial Action Task Force (FATF) has released its *Mutual Evaluation Report* for India, commending the country's efforts to implement robust measures against illicit finance, including money laundering and the financing of terrorism (ML/TF). The report highlights that India has attained a high level of technical compliance with the FATF recommendations. Accordingly, India has been placed under the "regular follow-up" category, which represents the highest rating tier assigned by FATF. Among the G20 nations, only the United Kingdom, France, and Italy—along with India—have received this recognition.

As outlined in the report, NABARD is expected to continue strengthening its understanding of ML/TF risks, as well as enhancing its supervisory capacity. This is to be achieved through ongoing training initiatives and increased engagement with other regulatory bodies, such as the RBI.

7.3 OTHER SUPERVISORY INITIATIVES

7.3.1 Fraud monitoring and KYC/AML[2]

To enhance the effectiveness of fraud monitoring and review, NABARD issued the following policy directives:

- Policies on monitoring fraud risk management in SEs.
- Policies on monitoring and examining KYC, AML, and CFT/CPF frameworks in SEs.

1. **Collaboration and meetings**
   a. Financial sector regulators meetings: NABARD actively participated in meetings of financial sector regulators held in New Delhi. These deliberations focused on the status of AML software implementation, NABARD's induction into the FPAC, and the signing of an MOU with FIU-IND.
   b. FPAC: NABARD recently became a member of the FPAC platform established by FIU-INDIA. This initiative facilitates ongoing collaboration between FIU-INDIA and various stakeholders involved in AML/CFT efforts.

c. MOU with FIU-IND: NABARD and FIU-IND executed an MOU on 3 September 2024 to enable:
   i. exchange of relevant intelligence and information available in respective databases;
   ii. conduct of outreach and training programmes for SEs; and
   iii. organisation of quarterly meetings and appointment of a nodal officer, among other measures.

2. **CKYC records registry awareness**: CERSAI organised three awareness programmes on the CKYC Records Registry at Siliguri, Jabalpur, and BIRD, Mangaluru on 10 May 2024, 20 May 2024, and 3 June 2024, respectively. NABARD officers addressed participants on various dimensions of KYC, AML, and CFT compliance.
3. **Cyber fraud prevention**
   a. Cyber frauds involving money mules are increasingly targeting RRBs and RCBs amid growing digitalisation in the financial sector.
   b. To counter these threats, NABARD is actively collaborating with the I4C under the Ministry of Home Affairs, as well as the RBI. Key initiatives include:
      i. dissemination of RBI advisories concerning the use of money mule accounts for cyber-enabled frauds to RRBs and RCBs;
      ii. encouraging SEs to register on the "Suspect Registry" maintained by I4C; and
      iii. conducting sensitisation programmes for SE officers, in collaboration with I4C, on the generation of alerts and the requisite follow-up actions.

7.3.2 Capacity building

Bank supervision is a highly specialised domain, and IOs must be trained to "see through the fog in times of crisis" and to "sense distress well in advance." Accordingly, several capacity-building initiatives were undertaken during FY2025.

1. **Senior Supervisory Managers (SSMs) Programme**: In collaboration with the College of Supervisors (COS), RBI, the National Bank Staff College (NBSC), Lucknow organised a dedicated programme for SSMs of NABARD on 4–6 November 2024, Mumbai. The programme aimed to strengthen the SSM function and enhance the capabilities of SSMs and their teams within NABARD. A total of 35 officers (comprising 26 SSMs and 9 other officers from Head Office and technical establishments) attended the programme.
2. **Training programmes at COS, RBI**: During FY2025, 54 officers participated in 32 programmes conducted by the COS, RBI. These covered a broad range of topics including supervision, risk management, data analytics, econometrics, application of advanced tools for analysis of supervisory and raw data, governance, report writing, leadership, communication, financial statements, and fintech.

7.3.3 Complaints Management System

The Complaints Management System (CMS) module was launched on 1 April 2022 to facilitate the seamless transmission of complaints to regional offices, enable effective monitoring and resolution of complaints, and support the generation of MIS reports.

With effect from 1 April 2025, the Centralised Public Grievance Redress and Monitoring System portal was adopted on a full-fledged basis by NABARD to ensure the effective resolution and management of grievances and complaints received against SEs.

7.3.4 References from Enforcement Department, RBI

The RBI established the Enforcement Department (EFD) in 2017 to ensure regulatory compliance and undertake enforcement actions against various Regulated Entities of the RBI. The EFD also issues Show Cause Notices and Speaking Orders to SEs of NABARD, namely RRBs, StCBs, and DCCBs (Figure 7.3).

Figure 7.3: Enforcement actions taken during FY2025

	RRBs	StCBs	DCCBs	Grand total
No. of SOs issued	7	6	53	66
Penalty imposed (in ₹ lakh)	58.9	26	129.2	214.1

DCCB = District Central Cooperative Bank, RRB = Regional Rural Bank, SO = Speaking Order, StCB = State Cooperative Bank.

7.4 INFORMATION TECHNOLOGY AND CYBER SECURITY INITIATIVES[3]

To enhance the monitoring of cyber security preparedness across SEs, the CSITE Cell, established in NABARD in 2018, undertook several initiatives during FY2025.

1. **Expanding human resources in CSITE**: The CSITE Cell was augmented with the induction of six external consultants. This enabled the expansion of IT/IS examinations to cover a greater number of SEs, facilitated desk-based scrutiny of VICS returns, supported the examination of compliance submissions by SEs in response to IT/IS findings, allowed for the timely issuance of alerts and advisories, and enhanced the handling of other critical functions of CSITE.
2. **Operationalisation of IT/IS examinations**: The Board of Supervision, at its 88th meeting, approved the operationalisation of IT/IS examinations of RRBs and RCBs, based on their digital maturity and degree of integration with the payments ecosystem. The objective of these examinations is to assess the cyber security framework of SEs through scrutiny of:
   a. IT/IS and cyber security policies;
   b. adequacy of the frameworks;
   c. functioning of relevant committees;
   d. implementation of prescribed cyber security controls based on entity classification; and
   e. compliance with advisories and alerts issued by RBI, NCIIPC, CERT-In, and IDRBT.

   During FY2025, 38 SEs (including 20 RRBs, 9 StCBs, and 9 DCCBs) were taken up for IT/IS examination by the NABARD Head Office; additionally, regional offices conducted IT/IS examinations of 35 DCCBs.
3. **Cyber Security Awareness Month**: CSITE observed Cyber Security Awareness Month in October 2024, during which the following activities were conducted:
   a. webinar for top management (Chairperson/CEO/MD) of SEs;
   b. cyber security session at NABARD, Head Office for Heads of Department, CTO, and CISO;
   c. webinar for faculty members of Cooperative Training Institutes;
   d. one-day workshop at BIRD, Mangaluru for CISOs of SEs;
   e. workshop at NBSC, Lucknow for NABARD's IOs;
   f. issuing of a guidance note for conducting IT/IS examinations;
   g. dissemination of digital content on cyber security including:
      i. *Cyber Security Handbook* for SEs; and
      ii. "31 Days' Challenge" to enhance cyber security awareness among SE staff.

4. **Capacity-building through cyber security awareness workshops**: CSITE provided faculty support for 28 virtual and 3 physical cyber security workshops. Of these, 26 were conducted for SEs on cyber security best practices, and 5 were targeted at regional offices for capacity building in IT/IS examination.
5. **High-level engagement**: CSITE engaged in eight high-level meetings with agencies such as the I4C, CERT-In, and MHA, ensuring it remained abreast of emerging cyber threats. The participation of senior officers from CSITE in these meetings underscored NABARD's commitment to addressing digital fraud and improving the cyber resilience of SEs.
6. **Advisories issued to SEs on enhancing cyber security measures**: Various circulars were disseminated to SEs to strengthen cyber security measures, including:
   a. Cyber security audit: SEs were advised to follow MeitY's guidelines for conducting regular cyber security audits of their IT infrastructure, websites, and applications (including APIs), especially upon system changes, using CERT-In empanelled agencies.
   b. Vulnerability Assessment/Penetration Testing (VA/PT): SEs were advised to undertake vulnerability assessments for critical applications and applications in the DMZ on a half-yearly basis, and penetration testing on an annual basis, through CERT-In empanelled organisations.
   c. Sharing of common observations: CSITE shared common observations arising from IT/IS examinations and the scrutiny of VICS returns with all SEs.
   d. Cyber incidents and alerts: During FY2025, 60 cyber incidents were reported. CSITE issued 16 advisories/alerts to SEs, drawing from alerts/advisories issued by CERT-In, RBI, and other agencies.

7.5 WAY FORWARD

The following supervisory processes have been identified for implementation by NABARD during FY2025:

1. Capacity building of IOs across regional offices through the organisation of zonal workshops and specialised programmes in collaboration with NBSC and BIRD.
2. Capacity building of development assistants in partnership with NBSC.
3. Scaling up of IT/IS examinations to cover a greater number of SEs, with examinations of Level 1 and Level 2 entities conducted by regional offices, and those of Level 3 and Level 4 entities by the Head Office.
4. Regular updating of existing guidelines pertaining to the cyber security framework, IT/IS examinations, and audit processes applicable to SEs.
5. Automation of the IT/IS examination module.
6. Automation of the Alerts/Advisories module.

NOTES

1. C = Capital Adequacy, A = Asset Quality, M = Management, E = Earnings, L = Liquidity, S = Systems and Controls, C = Compliance.
2. Abbreviations used in this section: AML = Anti-Money Laundering, BIRD = Bankers Institute of Rural Development, CERSAI = Central Registry of Securitisation Asset Reconstruction and Security Interest of India, CFT = Combating the Financing of Terrorism, CKYC = Central Know Your Customer, CPF = Counter Proliferation Financing, FIU-IND = Financial Intelligence Unit–India, FPAC = FIU-India Initiative for Partnership in AML/CFT/CPF, I4C = Indian Cyber Crime Coordination Centre, KYC = Know Your Customer, MOU = Memorandum of Understanding, RBI = Reserve Bank of India, RCB = Rural Cooperative Bank, RRB = Regional Rural Bank, SE = Supervised Entity.
3. Abbreviations used in this section: API = Application Programming Interface, BIRD = Bankers Institute of Rural Development, CERT-In = Indian Computer Emergency Response Team, CISO = Chief Information Security Officer, COE = Centre of Excellence, CSITE = Cyber Security and Information Technology Examination, CTO = Chief Technology Officer, DCCB = District Central Cooperative Bank, DMZ = Demilitarised Zone, I4C = Indian Cyber Crime Coordination Centre, IDRBT = Institute for Development and Research in Banking Technology, IO = Inspecting Officer, IS = Information System, IT = Information Technology, MeitY = Ministry of Electronics and Information Technology, MD = Managing Director, MHA = Ministry of Home Affairs, NCIIPC = National Critical Information Infrastructure Protection Centre, RCB = Rural Cooperative Bank, RBI = Reserve Bank of India, RO = Regional Office, RRB = Regional Rural Bank, SE = Supervised Entity, StCB = State Cooperative Bank, VICS = Vulnerability Index for Cyber Security.