

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 3

2026

© 2026 International Journal of Law Management & Humanities

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of any **suggestions or complaints**, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to submission@ijlmh.com.

Digital Blind Spot: How the 2025 Banking Laws (Amendment) Act Overlooks Technology Infrastructure Deficits in Cooperative Banks

BHUMIKA CHAWLA* AND ADITI MISHRA**

ABSTRACT

The integration of modern technology in cooperative banking marks a significant shift in how these community-based financial institutions operate and serve their members. Traditionally known for their localized, member-centric approach, cooperative banks are now embracing digital innovations to enhance efficiency, transparency and inclusivity. The Banking Regulation (Amendment) Act, 2025 (Act No. 16 of 2025) seeks to strengthen governance, capitalization and oversight of cooperative banks in India to prevent a bigger crisis, non-performing assets and risks that could affect the whole system, improve depositor protection and enhance supervisory oversight of cooperative banks in India. However, the act overlooks the significant technology infrastructure deficits affecting these institutions such as outdated core banking systems, inadequate cybersecurity frameworks and limited digital adoption - which continue to hinder regulatory compliance and operational resilience. Findings reveal a policy gap: while the Act introduces managerial reforms, it fails to address technology deficits that amplify operational vulnerabilities, potentially undermine financial inclusion goals. By identifying this as a structural flaw, the study proposes amendments including mandatory IT infrastructure and RBI-led digital transformation. With the right blend of policy support and these recommendations cooperative banks can evolve into technology-capable institutions that remain their member-centric character while meeting contemporary compliance and security channels while ensuring cooperative banks sustainability.

Keywords: Banking Laws (Amendment) Act 2025, Cooperative Banks, Technology Infrastructure, Cybersecurity, Digital Financial Inclusion, RBI Regulatory Framework

* Author is a Student at Quantum University, Roorkee, Uttarakhand, India.

** Author is an Assistant Professor (Law) at Quantum University, Roorkee, Uttarakhand, India.

I. INTRODUCTION

Cooperative banks have long served as vital pillars of financial inclusion, particularly in rural and semi-urban areas, by promoting self-help, mutual assistance and community based economic development. Rooted in democratic governance service, these institutions have historically catered to the needs of farmers, small entrepreneurs, artisans and governance and development models have historically focused on the needs of economically marginalized members. However, the evolving landscape of global finance, marked by rapid technological advancement, has compelled cooperative banks to modernize their operations. The digital revolution encompassing innovations like artificial intelligence, blockchain, cloud computing, mobile technology, presents both unprecedented opportunities and significant challenges for the cooperative banking sector. Embracing these technologies is no longer optional but essential for survival, competitiveness, and relevance in an increasingly interconnected and digitalised financial ecosystem.

Cooperative banking plays an extremely important role in contributing to various aspects of the development of the agricultural and rural economy. Compared with scheduled commercial banks, there is a need to strengthen the process to improve various aspects of governance, especially to improve the technological adoption. Only about a quarter of Primary Agricultural Credit Societies (PACS) are truly digitalized, exposing major tech lags in cooperative banks. Most still use manual or fragmented systems, lack full CBS/ERP, offer limited UPI and digital payments, and have weak MIS and cybersecurity. Capital constraints, poor connectivity, low digital literacy, limiting scale and integration challenges slow digital rollout despite ongoing government computerisation schemes.

The Banking Laws (Amendment) Act, 2025 (Act No. 16 of 2025) introduces governance reforms across five banking statutes, with cooperative-bank-specific provisions addressing director tenures, nomination rules and reporting cycles. Yet, the act sidelines technology infrastructure deficits that critically undermine cooperative banks viability. Recent incidents, such as the July 2024 ransomware attack on C-Edge Technologies Ltd., a joint venture between Tata Consultancy Services and State Bank of India serving approximately 300 cooperative and Regional rural banks, which disrupted UPI, NEFT, and ATM services across the sector – underscore this vulnerability.¹ The 2025 Act's focus on financial metrics, ignores these tech gaps, creating a regulatory blind spot.

¹ Nat'l Payments Corp. of India, Statement on C-Edge Technologies Ransomware Attack (July 31, 2024); NPCI Re-establishes Connectivity with C-Edge After Ransomware Attack, Bus. Standard (Aug. 1, 2024),

II. SURVEYING PRIOR SCHOLARSHIP

Technology has become an increasingly central concern in the governance of cooperative banks in India. A growing body examines the promise and limitations of digital transformation in the sector. This section critically organises the literature across three areas – technology adoption and its uneven reach, governance and financial limitation, and regulatory responses to institutional failure.

A. Technology Adoption and the Last-Mile Problem

The transformative prospective of digital technologies for cooperative banking is well established in recent scholarship. Abraham and Singh contend that artificial intelligence, blockchain, and mobile banking carry the capacity to improve operational efficiency, financial inclusion outcomes, and governance mechanisms in cooperative banks, and argue that tactical technology adoption is no longer discretionary for institutions seeking to remain competitive in India's digital financial ecosystem.² Sindu M. demonstrates through an examination of digital platform incorporation in Indian cooperative banks that Core Banking Solutions, mobile banking interfaces, and payment systems such as UPI have materially improved rural engagement and operational regulation where they have been adopted, while also documenting the sharp separating in adoption between Urban Cooperative Banks, approximately 95% of which operate on CBS, and Primary Agricultural Credit Societies, of which only around 25% have achieved comparable integration.³ Kaurav similarly documents the potential of blockchain, fintech partnerships, and mobile banking to strengthen cooperative society governance and transparency, while admitting that limited funds, digital illiteracy, and cybersecurity risks constrain adoption in practice.⁴

These three studies establish a scholastic accord: technology adoption in cooperative banking is beneficial, demonstrably practical, and urgently needed. However, a critical gap runs through all three. None interrogates the role of the regulatory framework in dictating, stimulating, or obstructing that assumption. The implicit assumption is that barriers to digital transformation are primarily operational and financial in nature. What remains unexamined is whether India's legislative planning for cooperative banking requires technology adoption at all, and what

https://www.business-standard.com/finance/news/npci-reestablishes-connectivity-with-c-edge-following-ransomware-attack-124080101552_1.html.

² Roy Abraham & Kuldip Singh, Modernizing Cooperation: The Role of Technology in Cooperative Banking, 8 Int'l J. Rsch. & Tech. 59, 59-71 (2025).

³ Sindu M., Exploring the Integration of Digital Platforms in Cooperative Banks: An Examination of Innovation and Inclusion, 3 The Academic 539, 539-546 (2025).

⁴ Prashant Kaurav, Technological Advancements in Cooperative Societies: Opportunities and Challenges, 1 Innovative Horizons J. 16, 16-22 (2025).

repercussion follow from legislative silence on this question. The present study addresses precisely that gap.

B. Governance Constraints, Financial Vulnerabilities, and the Technology–Governance Nexus

Second strand of focuses on the structural restrictions limiting cooperative banks' operational effectiveness, with technology identified as among several unified deficits. Devika J. and Misha Davis A., drawing on primary data from Urban Cooperative Banks in Kerala, identify high non-performing assets, regulatory complexity, inadequate staff training, and limited technology investment as overlapping restrictions on fund and investment management, recommending technological adoption alongside improved training and policy reform.⁵ Prakash and Yadav, examining district central cooperative banks in Haryana, identify the same bunch of vulnerabilities, limited technology, high NPAs, inadequate staff capacity, and similarly recommend technology adoption and infrastructure investment as remedial measures.⁶

Both studies establish that the technology deficit in cooperative banking is structurally tangled with broader governance and financial weaknesses. However, both share the limitation noted above: they recommend technology adoption as a policy solution without examining whether the existing legislative framework supports or requires it. The present study brings these two strands into direct contact by asking whether the Banking Laws (Amendment) Act, 2025 creates any regulatory obligation or incentive structure that would address the deficits.

C. Regulatory Failure, Institutional Collapse, and Technology as a Structural Variable

The most directly relevant strand concerns the analysis of major cooperative bank failures and their regulatory repercussions. Shakeel, Siddiqui, and Siddiqui examine the collapse of Punjab and Maharashtra Cooperative Bank in 2019 as a case study in corporate governance failure, focusing on the inadequacy of board oversight, the absence of effective supervisory response, and the structural weaknesses of the framework governing cooperative banks.⁷

The PMC Bank collapse was not only a governance failure, it was a technology failure that governance mechanisms alone could not have detected or prevented. The creation of over

⁵ Devika J. & Misha Davis A., Suggested Strategic Solutions to the Constraints in Funds and Investment Management of Urban Co-operative Banks, 43 Asian J. Agric. Extension, Econ. & Soc'y 154, 154-162 (2025)

⁶ Jai Prakash & Priyanka Yadav, Assessing the Status of IT Initiative in District Central Co-operative Banks: Evidence from Haryana, 2 Int'l J. Advanced Rsch. & Multidisciplinary Trends 357, 357-369 (2025).

⁷ Mohd Raagib Shakeel et al., PMC Bank Debacle: A Failed Corporate Governance Case, S. Asian J. Bus. & Mgmt. Cases (2025), <https://doi.org/10.1177/25166042241274843>.

21,000 fictitious accounts to conceal HDIL-linked loan exposure of approximately ₹6,226 crore was structurally possible only in the absence of a real-time Core Banking Solution.⁸ RBI's supervisory mechanisms were defeated not simply because of weak governance but because the bank's technology infrastructure made systematic protection feasible. Reframing PMC Bank from a governance failure to a technology-enabled governance failure has direct implications for evaluating the adequacy of the 2025 Act's governance.

D. Research Gap

While existing strands establishes both the scope of technology deficits in cooperative banking and the governance improvements introduced by legislative interventions, no study has systematically examined whether the Banking Laws (Amendment) Act, 2025, the most substantive regulatory reform enacted since the PMC Bank crisis, adequately addresses those technology deficits. The literature reviewed above either treats technology adoption as an operational challenge, or examines governance failures without emphasizing technology infrastructure as an independent variable. This study addresses that gap through doctrinal analysis of the Act's provisions, situating statutory text against empirical data on technology adoption rates, cybersecurity incidents, and compliance across the cooperative banking sector.

III. METHODOLOGICAL APPROACH

This study uses doctrinal legal research methodology to analyze the Banking Laws (Amendment) Act, 2025 and its treatment of technology infrastructure obligations in cooperative banking sector. Doctrinal analysis involves the systematic analysis of legislative texts, statutory provisions, and regulatory instruments to assess, and alignment with the conditions they are intended to govern.⁹ This methodology is appropriate to the present inquiry for two reasons. First, the paper's central research question, whether the 2025 Act adequately addresses technology infrastructure deficits in cooperative banks, is fundamentally a question about what the law provides and what it does not. Second, doctrinal analysis permits precise identification of regulatory silence: it is through sustained interview with the Act's text that the absence of technology-related mandates becomes analytically verifiable rather than merely asserted.

⁸ PMC Bank Disclosed Only Rs 439.6 Cr Exposure to HDIL of Rs 6,226 Cr: Report, Bus. Standard (Nov. 25, 2019), https://business-standard.com/article/current-affairs/pmc-bank-disclosed-only-rs-439-6-cr-exposure-to-hdil-of-rs-6-226-cr-report-119112501055_1.html; PMC Bank Created More than 21,000 Bogus Accounts to Hide Bad Loans to HDIL, Bus. Today (Dec. 30, 2019), <https://www.businesstoday.in/sectors/banks/pmc-bank-loaned-rs-50-crore-to-hdil-days-before-rs-6300-crore-scam-came-to-light/story/392866.html>.

⁹ Terry Hutchinson & Nigel Duncan, Defining and Describing What We Do: Doctrinal Legal Research, 17 Deakin L. Rev. 83, 84–85 (2012).

A. Analytical Framework

The doctrinal analysis is structured in three stages. In the first stage, the operative provisions of the Banking Laws (Amendment) Act, 2025 relevant to cooperative banks are identified and examined. These are principally Section 5 of the 2025 Act, which amends Section 16 of the Banking Regulation Act, 1949 to extend director tenures from eight to ten years, and Section 14, which amends Section 56 of the Banking Regulation Act, 1949 to standardise the fortnightly reporting cycle for cooperative banks.¹⁰ These provisions are read in the context of the Act's Statement of Objects and Reasons and official Ministry of Finance, which coherents the legislature's intentions. In the second stage, the provisions are examined not only for what they mandate but for what they are silent on, specifically, the absence of obligations relating to Core Banking Solutions, cybersecurity audits, artificial intelligence adoption, or rural digital infrastructure. Doctrinal analysis of legislative silence is an established method in legal scholarship: where a statute governs a regulated sector, the decision not to address a known and documented problem within that sector is itself a legally significant choice agreeable to critical scrutiny.¹¹ In the third stage, the regulatory gap identified through doctrinal analysis is triangulated against secondary empirical data drawn from institutional reports and documented incident records, in order to establish that the omission is not merely textual but carries material operational consequences for the sector the Act governs.

B. Source Selection and Authority

Primary legal sources include the Banking Laws (Amendment) Act, 2025 (Act No. 16 of 2025),¹² the Banking Regulation Act, 1949 (as amended),¹³ the Reserve Bank of India Act, 1934 (as amended),¹⁴ and the Gazette Notifications issued by the Ministry of Finance appointing commencement dates for the Act's provisions.¹⁵ These constitute the authoritative primary sources for the doctrinal analysis and are cited to the official Gazette of India.

¹⁰ Banking Laws (Amendment) Act, 2025, No. 16 of 2025, Gazette of India, Extraordinary, pt. II, § 1 (Apr. 15, 2025), §§ 5, 14.

¹¹ See generally Cass R. Sunstein, *Interpreting Statutes in the Regulatory State*, 103 Harv. L. Rev. 405, 446–48 (1989).

¹² Banking Laws (Amendment) Act, No. 16 of 2025, Gazette of India, Extraordinary, pt. II, § 1 (Apr. 15, 2025).

¹³ Banking Regulation Act, No. 10 of 1949, Gazette of India (Mar. 16, 1949) (India) (as amended through 2025).

¹⁴ Reserve Bank of India Act, No. 2 of 1934, Gazette of India (Mar. 6, 1934) (India) (as amended through 2025).

¹⁵ Ministry of Fin., GOV'T OF INDIA, Gazette Notification No. S.O. 3494(E), Gazette of India, Extraordinary, pt. II, § 3(ii) (July 29, 2025); Min. of Fin., Gov't of India, Gazette Notification, Gazette of India, Extraordinary (Dec. 9, 2025).

Secondary institutional sources include the RBI FREE-AI Committee Report (August 2025),¹⁶ NABARD's Annual Report 2023–24 and PACS computerisation data,¹⁷ and the RBI Report on Trend and Progress of Banking in India 2023–24.¹⁸ Sources were selected on the basis of three criteria: institutional authority, all postdate the PMC Bank crisis which are subsequent to the 2025 Act, and direct relevance. Case study material concerning the PMC Bank collapse and the C-Edge Technologies ransomware incident was drawn from RBI regulatory orders, Enforcement Directorate charge sheets, NPCI official statements, and peer-reviewed academic analysis.¹⁹

C. Limitations

Three principal limitations apply to this study. First, doctrinal research does not incorporate the perspectives of those subject to the law under examination. This analysis does not include primary data from cooperative bank practitioners, RBI supervisory officers, or rural depositors; a mixed-methods study incorporating structured interviews would materially enrich these conclusions.

Second, the 2025 Act is a recent enactment and implementation data is limited. The compliance impact assessments in Part IV are projections based on pre-existing infrastructure data, principally NABARD's PACS computerisation progress reports and the RBI FREE-AI Committee's survey findings, and not post-implementation audits of the Act's effects. Empirical revision of those assessments will be warranted as implementation progresses. Third, certain estimates used in Part IV are drawn from institutional sources that may themselves understate the extent of the problem due to reporting incentives embedded in government-produced data. These figures are used for illustrative purposes and are attributed to their institutional source throughout. Act's provisions and reviews cybersecurity incident data (2024 C-Edge ransomware) and case studies (PMC Bank).

IV. EXAMINING THE EVIDENCE

The Banking Laws (Amendment) Act, 2025 represents a meaningful regulatory evolution for cooperative banks, yet its provisions reflect a profound disconnect between governance-focused

¹⁶ Reserve Bank of India, Framework for Responsible and Ethical Enablement of Artificial Intelligence: FREE-AI Committee Report (Aug. 13, 2025), <https://www.rbi.org.in>.

¹⁷ Nat'l Bank for Agric. & Rural Dev., Annual Report 2023–24 (2024); Nat'l Bank for Agric. & Rural Dev., Digitalising Cooperatives: Computerisation of Primary Agricultural Credit Societies, <https://www.nabard.org/digitalizing-cooperatives.aspx> (last visited May 16, 2026).

¹⁸ Reserve Bank of India, Report on Trend and Progress of Banking in India 2023–24 (2024).

¹⁹ Nat'l Payments Corp. of India, Statement on C-Edge Technologies Ransomware Attack (July 31, 2024); NPCI Re-establishes Connectivity with C-Edge After Ransomware Attack, *Bus. Standard* (Aug. 1, 2024); Shakeel et al., *supra* note 7.

reform and the sector's documented technology infrastructure deficits. By looking closely at how policy changes actually affect people on the ground—rural connectivity voids, dreadful AI/GPU penetration, surging phishing in Primary Agricultural Credit Societies (PACS), and the cybersecurity vulnerabilities demonstrated by the 2024 C-Edge ransomware incident and the 2019 PMC Bank collapse - reveals not mere oversights, but a regulatory approach that does not engage with the sector's technology dimension.

A. Governance-First Amendments: What the Act Prioritises

Enacted amid persistent cooperative frailties post-PMC, the 2025 Act prioritizes structural stability sans digital scaffolding. Director tenures extend to a maximum 10 years (previously 8),²⁰ fostering "governance continuity" by curbing frequent turnovers that plague small boards; this aligns with the 97th Constitutional Amendment's professionalization ethos,²¹ aiming to retain institutional memory amid talent shortages. Nomination flexibility was expanded to allow up to four nominees per depositor-either simultaneously or successively-under Sections 10-13 of the 2025 Act and the Banking Companies (Nomination) Rules, 2025, effective 1 November 2025, replacing the earlier 1985 rules.²² Further, Section 14 of the 2025 Act standardises reporting to a uniform "Last day of the fortnight" cycle for all cooperative banks, replacing the earlier alternate-Friday system, effective 15 December 2025.²³ This is expected to improve the Reserve Bank of India's supervision through better and more timely monitoring using centralized systems.

However, the Act does not mandate the use of regulatory technology like API-based compliance systems, artificial intelligence for fraud detection, or advanced data tools. It also lacks clear standards for core banking systems, cybersecurity checks, or even basic digital infrastructure in rural areas. As a result, while the Act strengthens governance on paper, it does little to address the deeper digital weaknesses of the cooperative banking sector.

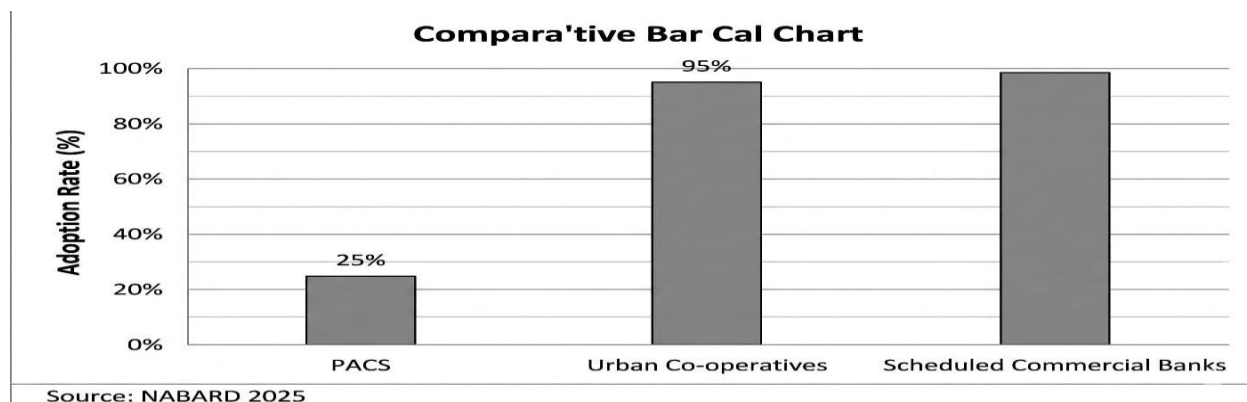
²⁰ Banking Laws (Amendment) Act, No. 16 of 2025, § 5 (amending Banking Regulation Act, No. 10 of 1949, § 16); Press Release, Press Info. Bureau, Min. of Fin., Gov't of India, Key Provisions of the Banking Laws (Amendment) Act, 2025 to Come into Effect from 1st August 2025 (July 30, 2025), <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2150371>.

²¹ The Constitution (Ninety-Seventh Amendment) Act, 2011, arts. 43B, 243ZH–243ZT (India).

²² Banking Laws (Amendment) Act, No. 16 of 2025, §§ 10–13; Banking Companies (Nomination) Rules, 2025, G.S.R. 790(E), Gazette of India, Extraordinary (Oct. 27, 2025) (effective Nov. 1, 2025).

²³ The Banking Laws (Amendment) Act, 2025, Is Set to Take Effect on December 15, 2025, INDIAN COOPERATIVE (Dec. 9, 2025), <https://www.cooperativebanks.in/rbi-guidelines/the-banking-laws-amendment-act-2025-is-set-to-take-effect-on-december-15-2025/>.

The Act contains no benchmarks for core banking solutions (CBS), cybersecurity audits, or rural broadband – a regulatory gap that leaves the sector's underlying digital vulnerabilities unaddressed.



B. Ground Realities: Connectivity Gaps and the AI Deficit

National Bank for Agriculture and Rural Development's 2025 findings show that rural cooperatives are still struggling badly with internet connectivity : About 40% of PACS do not have stable broadband, and only 25% are connected to Core Banking Solutions (CBS),²⁴ compared to nearly 95% in urban cooperatives; Jharkhand is far behind in digitization, with only 1,500 out of 4,454 PACS computerized in Phase I,²⁵ which slows down the spread of digital systems like UPI and AEPS. The RBI's FREE-AI Committee Report (August 2025) confirms a significant AI adoption gap in the cooperative banking sector. Among 264 Urban Cooperative Banks surveyed, only 16 reported deploying any AI tools, with no Tier 1 UCBs recording any adoption and Tier 2 and Tier 3 UCB adoption remaining below 10%.²⁶ The report attributes this lag to capacity constraints, high infrastructure costs, and limited business cases for AI integration in smaller-scale operations.²⁷

The system of reporting every two weeks assumes that banks already have digital systems, but rural PACS still depend on manual records, which slows down data sharing, increases compliance costs by 3 times, and leads to about 15% errors (as estimated by National Bank for Agriculture and Rural Development). The lack of AI also means these banks cannot predict bad loans early (unlike others that achieve up to 85% accuracy), leaving them stuck in reactive

²⁴ Nat'l Bank for Agric. & Rural Dev., Rural Cooperative Digitisation Report 2025 (2025), <https://share.google/CaAqsUOZKBHa9neIT>.

²⁵ Nat'l Bank for Agric. & Rural Dev., Jharkhand State Focus Paper 2024–25, at 42 (2024), <https://www.nabard.org>.

²⁶ Reserve Bank of India, Framework for Responsible and Ethical Enablement of Artificial Intelligence: FREE-AI Committee Report, at 23 (Aug. 13, 2025), <https://www.rbi.org.in>; RBI Panel Flags AI Gap in Co-op Banks, Moots Shared 'Landing Zones', INDIAN COOPERATIVE (Aug. 14, 2025), <https://www.indiancooperative.com/banks/rbi-panel-flags-ai-gap-in-co-op-banks-moots-shared-landing-zones/>.

²⁷ Reserve Bank of India, *supra* note 23, at 29.

problem-solving. This situation is not just simple neglect; it reflects serious regulatory failure in a digital payment.

C. Rising Cyber Threats and Vulnerability in PACS

Cyber fraud is spreading rapidly: phishing cases in PACS increased by 35% in 2024–25, reaching around 1,200 incidents and causing losses of nearly ₹150 crore.²⁸ This rise is mainly due to weak multi-factor authentication (MFA), lack of proper staff training, and the continued use of outdated SMS gateway systems. A clear example is the ₹11.55 crore cyber attack on Himachal Pradesh State Cooperative Bank in 2025,²⁹ where money was stolen through vulnerabilities in its mobile banking application.

There is no protection provided under the Act: the uniform fortnightly reporting system may actually increase risk, as unpatched systems remain exposed for longer periods, allowing large-scale phishing attacks to take place especially during data uploads to the RBI.

D. Case Studies: Cybersecurity Incidents and the PMC Bank Collapse

In July 2024, C-Edge Technologies Ltd., a joint venture between Tata Consultancy Services and State Bank of India that provides core banking and payment infrastructure to cooperative and regional rural banks, suffered a ransomware attack attributed to the Ransom Exx group.³⁰ NPCI isolated C-Edge from its retail payment systems as a preventative measure, disrupting UPI, NEFT, RTGS, and ATM services for customers of approximately 300 cooperative and regional rural banks for nearly two days.³¹ NPCI subsequently confirmed that the attack was contained within C-Edge's own data centre and did not compromise the infrastructure of the cooperative banks themselves.³² The incident nonetheless exposed the structural vulnerability of cooperative banks that depend on shared third-party technology infrastructure operating without statutory minimum security standards.

The collapse of Punjab and Maharashtra Cooperative Bank in 2019 involved HDIL-linked loan exposure of approximately ₹6,226 crore-admitted by the bank during RBI inspection as of 31

²⁸ Indian Comput. Emergency Response Team, Annual Report 2024, at 7–8 (2024), <https://www.cert-in.org.in>.

²⁹ Press Release, Reserve Bank of India, RBI Imposes Monetary Penalty on The Himachal Pradesh State Co-operative Bank Ltd., Himachal Pradesh, Press Release 2026-2027/98, <https://www.rbi.org.in>.

³⁰ NPCI Re-establishes Connectivity with C-Edge After Ransomware Attack, Bus. Standard (Aug. 1, 2024), https://www.business-standard.com/finance/news/npci-reestablishes-connectivity-with-c-edge-following-ransomware-attack-124080101552_1.html.

³¹ Nat'l Payments Corp. of India, Statement on C-Edge Technologies Ransomware Attack (July 31, 2024).

³² Id.

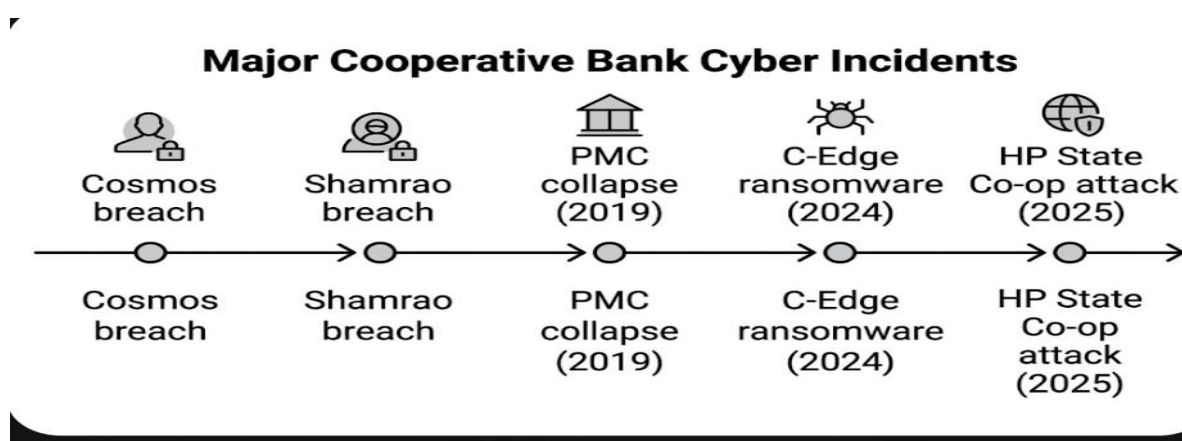
March 2019-against total advances of ₹8,383 crore, representing approximately 74% of its loan book.³³

This crisis happened largely due to lack of proper technology systems. The bank did not have a core banking system (CBS) that could track loans in real time. Thousands of fake or hidden accounts were created—21,049 compared to just 44 genuine ones—to hide bad loans and avoid detection during audits. The Reserve Bank of India remained unaware of the true situation until whistleblowers revealed the fraud. Official reports showed non-performing assets (NPAs) at only 2.19%,³⁴ which was far lower than the actual level, as the losses were deliberately hidden through weak systems and poor monitoring.

The Banking Laws (Amendment) Act, 2025 strengthens governance in cooperative banks, but its focus remains largely administrative, leaving technological weaknesses insufficiently addressed. Provisions such as extended director tenures, flexible board nominations, and periodic reporting aim to improve oversight; however, they implicitly assume the existence of adequate digital infrastructure, which many cooperative institutions still lack.

Past instances demonstrate that governance failures are often intertwined with technological deficiencies rather than existing in isolation. Moreover, compliance mechanisms like regular reporting become less effective where digital connectivity and automated systems are inadequate.

Thus, while the Act fortifies governance frameworks, its limited engagement with technological resilience renders it incomplete, highlighting the need to integrate digital safeguards as a core component of regulatory design.



³³ PMC Bank Disclosed Only Rs 439.6 Cr Exposure to HDIL of Rs 6,226 Cr: Report, Bus. Standard (Nov. 25, 2019), https://business-standard.com/article/current-affairs/pmc-bank-disclosed-only-rs-439-6-cr-exposure-to-hdil-of-rs-6-226-cr-report-119112501055_1.html.

³⁴ Id.

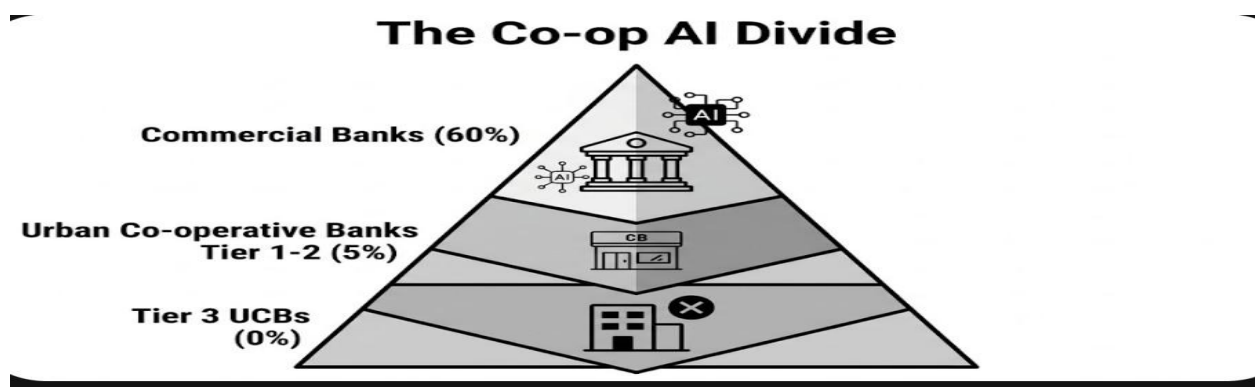
V. CRITICAL ANALYSIS: LIMITATIONS, ASSUMPTIONS, AND ALTERNATIVE VIEWS

The scale of the digital divide proved more severe than initially anticipated. NABARD's 2025 findings confirmed that nearly 40% of PACS lack stable broadband access, and only 25% are connected to Core Banking Solutions (CBS), compared to 95% in urban cooperatives.

In Jharkhand alone, only 1,500 out of 4,454 PACS were computerized even after Phase I of digitization efforts.

The RBI's FREE-AI Committee Report (2025) showed that less than 5% of cooperatives use AI or advanced computing tools. Among Tier 3 Urban Cooperative Banks, this figure stands at 0%, while commercial banks average around 60% AI adoption. Setup costs of ₹10–50 crore per institution, shortage of skilled staff, and unreliable electricity were identified as the main barriers, creating what the report describes as the "coop AI divide."

These findings required reconsideration of the initial assumption that the problem was exclusively one of regulatory design. It revealed a structural, resource-driven crisis that law alone cannot fix overnight. The PMC Bank collapse (2019) was particularly difficult to analyze objectively. The bank had 21,049 fake or hidden accounts compared to just 44 genuine ones, masking a ₹4,355 crore fraud linked to HDIL, representing roughly 73% of its total loan book. The RBI remained unaware until whistleblowers came forward, and official NPA reports showed only 2.19%³⁵, drastically understating the true level of distress.



What struck most was that this was not just a governance failure, it was a technology failure. The absence of a real-time CBS meant fraudulent accounts could be created and concealed for years. The analysis had to resist the temptation to frame this purely as a moral failure of bank directors and instead examine the systemic digital void that made the fraud possible and invisible.

³⁵ Reserve Bank of India, Inspection Report on Punjab and Maharashtra Cooperative (PMC) Bank (Sept. 2019).

Similarly, the 2024 C-Edge ransomware attack, which paralyzed 200+ cooperative banks, exposed 1.5 lakh customer records, and disrupted NEFT, RTGS, and UPI transactions worth nearly ₹5,000 crore³⁶, was analyzed carefully. The attack succeeded largely because banks were running outdated servers without proper encryption.

Historical breach data further reinforced this: the Cosmos Bank breach (₹94 crore)³⁷ and the Shamrao Vithal Cooperative Bank breach showed that this is a pattern, not an isolated incident. This paper examines the significance of the Act's silence too.

The Act makes no mention of:

- API-based compliance systems
- AI tools for fraud detection
- Cybersecurity audit requirements
- Core banking solution benchmarks
- Rural broadband mandates

It would be easy, and perhaps unfair, to treat every silence as negligence. The paper considers the possibility that the legislature intended these matters to be addressed through RBI circulars and subordinate regulation, rather than the parent Act. However, given the 35% rise in phishing attacks on PACS in 2024–25 (reaching approximately 1,200 incidents and causing losses of nearly ₹150 crore), and the ₹11.55 crore cyberattack on Himachal Pradesh State Cooperative Bank in 2025 through its mobile banking application, this paper concluded that leaving cybersecurity to discretionary circulars creates dangerous enforcement gaps. This interpretive choice has been made transparent in analysis so readers can evaluate whether they agree.

One methodological choice made in this study was to quantify the compliance burden wherever possible, rather than leaving impact assessments vague. For example:

Rural PACS relying on manual records face 3x higher compliance costs and approximately 15% data errors when meeting the Act's uniform fortnightly reporting requirement, as estimated by NABARD.³⁸ The fortnightly reporting cycle assumes banks already have digital infrastructure, yet 60% of rural transactions are only now becoming digital, meaning the compliance burden falls hardest on the least-equipped institutions.

³⁶ Press Release, Nat'l Payments Corp. of India, Public Advisory: Temporary Isolation of C-Edge Technologies from NPCI Retail Payment Systems (July 31, 2024), <https://www.npci.org.in>.

³⁷ Pune Court Convicts 11 Accused in Cosmos Bank's Rs 94 Cr Cyber Fraud Case, *Bus. Standard* (Apr. 23, 2023), https://www.business-standard.com/india-news/pune-court-convicts-11-accused-in-cosmos-bank-s-rs-94-cr-cyber-fraud-case-123042300456_1.html.

³⁸ Nat'l Bank for Agric. & Rural Dev., *Cooperative Banking Review* 2025, at 45–48 (2025).

These numbers help avoid vague claims and ground the critique in measurable terms. However, it is acknowledged that some of these figures come from government-produced reports, which may themselves understate problems due to reporting incentives.

Three key limitations in the positionality of this study are:

- First, the study analyses a very recent Act (2025) with limited longitudinal data on its actual implementation. The compliance impact assessments are largely projections based on existing infrastructure data, not post-implementation audits.
- Second, the paper's focus on technology gaps may inadvertently downplay the genuine governance improvements the Act introduces, such as director tenure stability, the 97th Constitutional Amendment alignment, and improved nomination rules under the Banking Companies (Nomination) Rules, 2025. These are real gains that rural depositors will benefit from.
- Third, the doctrinal framework does not capture the voices of cooperative bank staff, rural depositors, or RBI officers who administer these rules. A mixed-methods study incorporating interviews would strengthen the conclusions significantly.

Legal reform, however well-intentioned, must be stress-tested against the weakest point in the system it governs. The Banking Laws (Amendment) Act, 2025, strengthens the roof of cooperative banking governance, but the floor, made of crumbling digital infrastructure, remains unaddressed. The analysis is shaped by this conviction. The analysis is shaped by this conviction and is presented through data, statutory text, and documented failures, while acknowledging that the Act is not without merit. The goal is not to condemn the legislature but to make a case that digital safeguards must become a core component of regulatory design, not an afterthought.

VI. CLOSING ARGUMENTS AND POLICY DIRECTION

The Banking Laws (Amendment) Act, 2025 arrives at a critical moment in India's financial history. Cooperative banks serve as the financial backbone of rural India, reaching farmers, small traders, and low-income depositors who have little access to commercial banking. Any legislation that strengthens this sector deserves recognition. And the Act does deliver meaningful governance reforms, longer director tenures, flexible nomination rules, and standardized fortnightly reporting are genuine improvements that will bring more stability and accountability to cooperative bank management.

But governance reforms alone cannot protect a bank that can be paralyzed by a ransomware attack overnight.

This is the central finding of this research. The Act prioritises governance reforms-director tenures, nomination rules, and reporting standardisation-while leaving technology infrastructure requirements entirely unaddressed. A governance framework operating on top of deficient digital infrastructure cannot by itself ensure institutional safety or regulatory compliance. It addresses the symptoms of institutional failure while leaving the deeper technological causes unregulated and unresourced.

This is not merely an oversight, it represents a regulatory paradigm that is dangerously misaligned with India's digital financial reality, where nearly 60% of rural transactions are now conducted digitally every year.

The following policy recommendations are offered in the spirit of completing what the 2025 Act began, building cooperative banks that are not only well-governed, but digitally resilient, cybersecure, and genuinely capable of serving rural India in the 21st century.

- **Mandate Core Banking Solutions for All Cooperative Banks**

The single most impactful reform would be making CBS non-optional. The PMC Bank fraud was only possible because loan accounts could be hidden from supervisors in the absence of real-time tracking. CBS eliminates this blind spot entirely.

Banks that fail to comply should face restrictions on deposit acceptance, a consequence serious enough to drive action.

- **Create a Dedicated Cooperative Bank Cybersecurity Framework**

The RBI's existing cybersecurity guidelines were designed primarily for commercial banks and scheduled banks. Cooperative banks, with their weaker IT teams, older infrastructure, and rural connectivity challenges, need a separate, tiered framework calibrated to their actual capacity.

- **Establish a Rural Digital Infrastructure Fund under NABARD**

40% of PACS without broadband is not a technology problem, it is a public investment problem. Private banks invested in their own digital infrastructure because it was profitable. Rural cooperatives cannot do the same, and the market will not do it for them.

Parliament should establish a dedicated Rural Cooperative Digital Infrastructure Fund under NABARD, funded through a small cess on commercial bank profits or direct budgetary allocation.

- **Amend the Act to Include Mandatory Technology Audit Provisions**

The 2025 Act should be amended, or supplemented through a Technology Regulation Schedule, to introduce statutory technology audit obligations alongside the existing financial audits. Just as the Act requires boards to maintain capital adequacy, it should require boards to maintain a minimum Technology Adequacy Score assessed annually by an independent auditor.

This score should evaluate CBS integration status, cybersecurity compliance level, AI/fraud detection tool adoption, staff digital literacy, and data backup and disaster recovery systems. Banks falling below the minimum score should receive a regulatory improvement notice, triggering a supervised remediation plan, not immediate penalties, which would disproportionately harm small rural banks.

- **Build an AI Adoption Roadmap for Cooperative Banks**

The RBI's FREE-AI Committee already identified the AI gap, less than 5% adoption in cooperatives versus 60% in commercial banks. What is missing is a concrete roadmap to close it. The RBI and Ministry of Cooperation should jointly release a Cooperative Bank AI Adoption Roadmap -- one AI platform serves multiple small banks through a cloud-based cooperative consortium, dramatically reducing per-bank costs.

- **Reform the Fortnightly Reporting Mandate to Be Infrastructure-Sensitive**

The Act's uniform fortnightly reporting requirement is well-intentioned but blunt. Applying the same reporting cycle to a fully digitized UCB in Mumbai and a paper-records PACS in rural Jharkhand is not uniform regulation, it is unequal burden.

The RBI should introduce a tiered reporting schedule: digitized banks report fortnightly as the Act requires; partially digitized banks report monthly with a CBS integration compliance plan attached; and manual-record banks report quarterly while receiving mandatory CBS onboarding support. This approach maintains the Act's supervisory intent while not penalizing banks for infrastructure gaps they cannot immediately overcome.

- **Strengthen Whistleblower Protections in Cooperative Banks**

The PMC Bank fraud was ultimately exposed not by the RBI's supervisory systems but by whistleblowers. Yet cooperative bank employees who raise internal fraud concerns have no statutory protection equivalent to those available in listed companies under SEBI regulations.

The Act should be amended to include an explicit whistleblower protection clause for cooperative bank employees, with anonymous reporting channels monitored by the RBI's Department of Supervision.

India's cooperative banks are not failing because their directors serve too few years or their nomination rules are too rigid. They are failing, and being attacked, defrauded, and digitally paralyzed, because decades of under-investment in technology have left them structurally vulnerable in a world that has gone almost entirely digital.

The Banking Laws (Amendment) Act, 2025 is a meaningful step forward in governance. But meaningful is not enough when 200 banks can be shut down by a single ransomware attack, when fraud worth thousands of crores can hide behind paper ledgers, and when 40% of rural cooperative societies cannot even access stable internet.

The next amendment must treat digital infrastructure not as a luxury for cooperative banks, but as the foundation without which no governance reform can succeed. The interests of rural depositors, who constitute the primary beneficiaries of the cooperative banking system, require that regulatory reform address governance and technology dimensions together rather than treating the latter as an afterthought.
