VOLUME 3, ISSUE 1 | JUNE 2026

The Banker

thebankermedia.com thebankermedia

media.com

Pg 54
VIEWPOINT
Vivek Gupta, Joint Director, National Federation of Urban Co-operative Banks and Credit Societies Ltd. (NAFCUB)

SPEED IS THE NEW SECURITY: WHY REAL-TIME FRAUD DETECTION HAS BECOME NON-NEGOTIABLE

DR. DEVDATTA CHANDGADKAR

The Leader Bridging Tradition and Technology

SIL
Formerly known as Saraswat Infotech Pvt. Ltd.

A BRAND OF BNG
bharatnetworkgroup.com

innovation is good™

Built for Banks that Power Bharat

India's Largest, Most Trusted and Comprehensive Lending Infrastructure for Banks

OPL helps banks move from legacy workflows to intelligent, standardized and high-volume digital credit delivery across MSME, retail and agriculture segments.

Powered by AI, data intelligence and straight-through processing, OPL enables banks to make faster and more consistent credit decisions.

With OPL, Banks can:

Make Sharper Credit Decisions
Evaluate MSMEs, thin-file and New-to-Credit borrowers with deeper intelligence.

Digitize Lending End-to-End
Simplifies the entire lending journey from application to approval, disbursement, and post-disbursement monitoring.

Scale Last-Mile Credit Confidently
Deliver faster lending with improved efficiency and stronger risk control.

Trusted Entity

Backed by institutional shareholding and a strong governance framework, OPL is trusted by leading financial institutions to power digital credit transformation and expand access to credit across Bharat.

+91 79 3500 3200 brijesh.mishra@oplinnovate.com www.oplinnovate.com

The Banker media.com

Your feedback about this magazine is welcomed at

editor@thefoundermedia.com

info@thefoundermedia.com

This magazine is published under/as a part of "HELLO FOUNDER INFOMEDIA PRIVATE LIMITED, an UTTAR PRADESH-based private limited company registered at the Ministry of Corporate Affairs (MCA). The Corporate Identification Number (CIN) of HELLO FOUNDER INFOMEDIA PRIVATE LIMITED is U56210UP2023PTC191833 and registration number is U56210UP2023PTC191833. HELLO FOUNDER INFOMEDIA PVT LTD's registered office address is Flat No 1006 10th Floor, Tulip 3 Gulmohar Garden, Raj Nagar Extension, Ghaziabad, Uttar Pradesh, India, 201017.

VOLUME 3, ISSUE 1 | JUNE 2026

Table of CONTENT

Ashish Srivastava (L) and Anupam Gupta (R), Founders, Bharat Network Group (BNG)

AI adoption is no longer optional for co-operative banks

Dear Prime Reader,

Co-operative banks sit at the last mile of India's financial system. They are where trust is most personal and where the consequences of fraud are most devastating. A customer who loses savings to a digital scam at a co-operative bank does not just lose money. They lose faith in an institution that may have served their family for generations.

That is what makes fraud resilience in this sector a matter of social responsibility, not just operational necessity. And that is why this edition of **The Banker Media Volume 3 Issue 1** takes the subject as seriously as it does.

This edition puts those institutions, and their leaders front and centre.

Their candour about the challenges they face and the progress co-operative banks are making is exactly the kind of conversation the sector needs more of.

INNOCRAZY

BANK COMMUNICATION PARTNER

INNOCRAZY

OUR SERVICES

- **AI ChatBots** – WhatsApp Banking
- **InnoRECON:** Reconciliation Solutions
- **InnoBOT:** AI Voice Calling Solutions
- **Bulk SMS API:** Fast & Secure
- **Inno RCS:** Multimedia Messages
- **Innocrazy Digital Media Marketing** for Lead Generation and Growth.

BOOK NOW

+91 7838666333, +91 8447799403

www.innocrazy.com

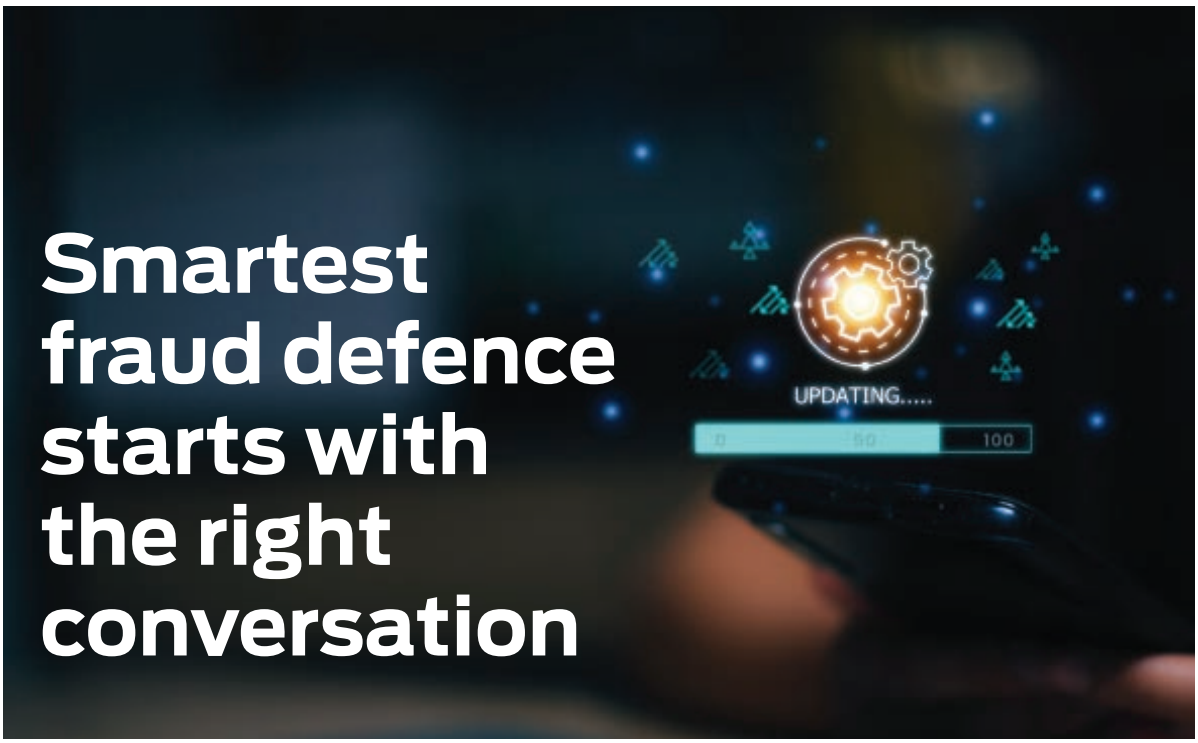
223 B Tower, ITHUM TOWER, Block A, Industrial Area, Sector 62, Noida, Uttar Pradesh

Trusted by 100+ BFSI & Businesses

www.innocrazy.com

Innocrazy Tech Services Private Limited

EDITOR'S CORNER



Smartest fraud defence starts with the right conversation

Dear Reader,

Fraudsters do not read annual reports. They do not care about asset size, branch count, or legacy. They look for gaps and right now, some of those gaps run straight through India's co-operative banking sector.

The Banker Media Volume 3 Issue 1 explores how these co-operative bank leaders are closing those gaps in real time either by deploying AI fraud layers, rethinking data privacy frameworks, modernising core banking integrations, or by building staff awareness that actually sticks.

What emerges is not a crisis narrative. It is a progress report from institutions that refuse to be left behind. Because when co-operative banks get stronger, India's financial fabric gets stronger too.

Here is to the leaders building that strength, one decision at a time.

Aishwarya Saxena
Sr. Associate Editor
editor@thefoundermedia.com

Co-operative banks are waking up to a new reality where trust alone is no longer enough

Speed is the new security: Why real-time fraud detection has become non-negotiable

Dr Devdatta Chandgadkar, CEO, SIL Infotech Pvt. Ltd. shares with **Aishwarya Saxena** why real-time fraud intelligence has become the most critical investment a bank can make right now

Given SIL's deep roots in co-operative banking, how different is the sales motion and product expectation of a co-operative bank versus a commercial bank and how has that shaped SIL's go-to-market approach?

The expectations and operating realities of co-operative banks are fundamentally different from those of large commercial banks. Co-operative banks typically operate with deep community relationships, strong regional influence, and a customer base that values trust, accessibility, and personalised service. However, many of these institutions also face challenges such as limited technology budgets, smaller IT teams, legacy infrastructure, and evolving regulatory requirements. Commercial banks, on the other hand, usually have larger technology teams, established digital ecosystems, and faster adoption cycles for enterprise-grade innovation.

At SIL, our roots in co-operative banking helped us understand these realities from the ground up. Instead of building products only for large urban banking institutions, we focused on creating scalable and modular

platforms that are practical, affordable, and easy to deploy for banks of every size. Our go-to-market approach has therefore been highly consultative rather than transactional.

For co-operative banks, the sales motion is centered around partnership, handholding, and long-term transformation. We spend significant time understanding the operational workflows of the bank, regulatory compliance needs, customer demographics, and digital maturity levels before recommending solutions. In many cases, banks require not only technology implementation but also guidance around digital adoption, process redesign, and customer onboarding strategies.

This understanding shaped SIL's product philosophy. Our platforms are designed to reduce complexity while enabling banks to rapidly adopt modern payment systems, digital banking capabilities, and AI-driven analytics. Whether it is UPI infrastructure, fraud monitoring, or analytics platforms, we ensure that the solutions remain interoperable, cost-efficient, and scalable.

At the same time, our experience working with co-operative banks has become a major strength even while engaging with larger commercial institutions. Large banks today also seek agility, faster deployment cycles, and localised innovation. SIL bridges this gap by offering enterprise-grade technology with the flexibility and responsiveness traditionally missing in the banking technology ecosystem.

SIL offers banks direct NPCI connectivity via SIL's UPI Switch. How do you price this capability, and

what does the commercial model look like for a bank processing ₹5 crore in monthly UPI volume?

SIL's UPI Switch is designed to help banks achieve direct NPCI connectivity while reducing dependency on intermediaries and improving operational control. Our pricing philosophy is based on scalability, sustainability, and alignment with the bank's transaction growth.

Typically, the commercial structure consists of three components: one-time implementation cost, annual platform support and maintenance, and transaction-based commercial models depending on volume and feature utilisation. The objective is to ensure that banks can start with a cost-effective deployment while benefiting from economies of scale as digital transaction volumes increase.

For a bank processing around ₹5 crore in monthly UPI volume, the engagement model is generally structured around transaction throughput, infrastructure requirements, fraud monitoring layers, reconciliation capabilities, and value-added integrations such as analytics or merchant services.

Beyond pricing, the real value proposition for banks lies in ownership and operational efficiency. Direct NPCI connectivity through SIL's UPI Switch enables banks to reduce latency, gain better visibility into transaction flows, improve reconciliation accuracy, strengthen fraud controls, and launch innovative digital products faster.

Additionally, SIL provides deployment flexibility through cloud-ready and on-premises models, allowing banks to align the solution with their internal governance and compliance frameworks. As UPI adoption continues to accelerate across urban and rural India, banks increasingly recognise that

> **Our systems are designed to operate in real time so that banks can proactively identify suspicious activity before financial damage occurs**

payment infrastructure is not merely a compliance requirement but a strategic growth engine.

What data signals does SIL use as inputs for its fraud scoring, is it transaction history, device fingerprinting, geolocation, or something else?

Fraud prevention in today's digital banking ecosystem requires a multi-layered and intelligence-driven approach. At SIL, our fraud scoring framework is designed to combine behavioural analytics, transaction intelligence, contextual signals, and AI-driven anomaly detection.

Transaction history is one of the primary inputs because it helps establish customer behaviour patterns over time. However, modern fraud detection cannot rely on transaction history alone. SIL's fraud intelligence models also evaluate device fingerprinting, geolocation patterns, login behaviour, transaction velocity, beneficiary analysis, session activity, and network-based correlations.

For example, if a transaction originates from an unusual location, on a new device, and with a sudden increase in transaction value or frequency, the risk score dynamically increases. Similarly, repeated failed authentication attempts, suspicious merchant behaviour, abnormal transaction timings, and unusual beneficiary additions are treated as important indicators.

Our systems are designed to operate in real time so that banks can proactively identify suspicious activity before financial damage occurs. The objective is not only to block fraud but also to minimise false positives, ensuring that genuine customers continue to enjoy a seamless digital experience.

Another important aspect is

adaptive learning. Fraud patterns continuously evolve, particularly with the growth of instant payments and digital channels. SIL's AI-driven monitoring systems are therefore designed to learn from emerging fraud behaviour and continuously refine risk models.

Going forward, we also see stronger integration between fraud intelligence and customer analytics, where risk engines will increasingly become predictive rather than reactive. The future of fraud management will depend on intelligent orchestration of data, AI, and real-time decisioning.

PANORAMA is described as an AI analytics layer. What specific decisions does it help a bank's leadership team make that they could not make before?

PANORAMA was conceptualised to help bank leadership teams move from static reporting to intelligent decision-making. Traditionally, banks relied heavily on fragmented MIS reports, manual analysis, and retrospective data interpretation. While those systems provided visibility, they often lacked predictive capability and actionable intelligence.

PANORAMA changes this by consolidating operational, transactional, customer, and performance data into a unified AI-driven analytics framework. The platform enables leadership teams to

Most importantly, PANORAMA helps democratise data-driven decision-making within the organisation. Instead of depending solely on technical teams for reports, business leaders can access intuitive insights that improve speed, transparency, and strategic planning

One of the biggest advantages is predictive visibility. For instance, PANORAMA can help management identify branches with declining customer engagement, regions with rising digital adoption, or transaction patterns that indicate emerging fraud or operational inefficiencies. Instead of reacting after issues escalate, leadership teams can take preventive action early

identify trends, monitor risks, evaluate branch performance, understand customer behaviour, and make faster strategic decisions. One of the biggest advantages is predictive visibility. For instance, PANORAMA can help management identify branches with declining customer engagement, regions with rising digital adoption, or transaction patterns that indicate emerging fraud or operational inefficiencies. Instead of reacting after issues escalate, leadership teams can take preventive action early.

The platform also supports business growth decisions. Banks can analyse customer segmentation, product usage patterns, transaction frequency, and regional demand trends to improve product positioning and cross-selling strategies. This enables more targeted customer engagement and better allocation of resources.

Another major benefit is governance and compliance monitoring. Leadership teams gain real-time dashboards for operational oversight, allowing faster response to exceptions, risk indicators, and service-level deviations.

Most importantly, PANORAMA helps democratise data-driven decision-making within the organisation. Instead of depending solely on technical teams for reports, business leaders can access intuitive insights that improve speed, transparency, and strategic planning.

The Digital Rupee (e₹) pilot is underway in India. What role, if any, do you see SIL playing in the CBDC infrastructure stack and are there any specific product categories like lending-as-a-service, insurance distribution, CBDC integration, or credit bureau data that SIL is actively planning to enter in the next 2-3 years?

The Digital Rupee initiative represents a significant milestone in India's financial and digital payments evolution. While the ecosystem is still in the pilot and adoption phase, we believe CBDC infrastructure will eventually become an important layer within the broader banking and payments ecosystem.

SIL sees itself playing an enabling role in this transformation by helping banks integrate emerging digital currency capabilities into their existing banking infrastructure. Our expertise in payments, switching technology, interoperability, fraud monitoring, and digital transaction processing positions us well to support banks as CBDC adoption evolves.

We believe the long-term success of the Digital Rupee will depend not

only on issuance frameworks but also on seamless integration with banking systems, merchant ecosystems, customer onboarding journeys, security frameworks, and analytics platforms. SIL's focus will therefore remain on enabling scalable and secure infrastructure for participating banks.

Over the next two to three years, we also see strong opportunities across adjacent financial technology categories. AI-driven analytics, fraud intelligence, embedded banking capabilities, and advanced payment orchestration will continue to be major focus areas for us.

In addition, SIL is actively exploring opportunities around CBDC integration readiness, intelligent reconciliation systems, digital lending enablement, and deeper data-driven banking solutions. We also see increasing demand from banks for unified platforms that can combine payments, analytics, compliance monitoring, and customer engagement within a single ecosystem.

> **"At SIL, our roots in co-operative banking helped us understand these realities from the ground up**

India's banking transformation is entering a phase where technology providers must move beyond software delivery and become long-term innovation partners. SIL's vision is aligned with that future — building secure, scalable, and intelligent banking infrastructure that empowers institutions of every size to participate confidently in the next era of digital finance.

Banking on AI to beat fraudsters: A ground-level perspective on what really matters

Digital banking has opened new doors for customers and fraudsters alike. **Aishwarya Saxena** brings together **Avinash Alandkar, CEO, Laxmi Urban Co-operative Bank Pvt. Ltd., Ramlal Damodar Sanap, CEO, The Nashik District Urban Co-operative Banks Association Ltd., and JR Vishnoi, CEO, Rajsamand Urban Co-operative Bank**, for a candid conversation on how co-operative banks are fighting back

India's co-operative banks spent over a century doing the work larger banks would not. Farmers, small traders, towns with no branch for miles. That network now runs across 1,500 urban co-operative banks and nearly 96,000 village-level credit societies, according to the NABARD Annual Report 2024.

As of December 2024, urban co-operative banks collectively held assets worth over Rs 7.20 lakh crore, per RBI data presented in the Rajya Sabha. None of that insulates them from what is coming. UPI processed 21.7 billion transactions worth Rs 28.33 lakh crore in January 2026 alone, according to NPCI figures.

UPI volumes have grown from 92 crore transactions in 2017-18 to over 13,000 crores in 2023-24 and fraud

“At Laxmi Urban Co-operative Bank, we have shifted to quarterly, scenario-based training sessions for staff, including tabletop exercises focused on fraud patterns relevant to our region

Avinash Alandkar
CEO, Laxmi Urban
Co-operative Bank Pvt. Ltd.

has followed that curve. NPCI data recorded 6.32 lakh UPI fraud incidents in FY25, totalling Rs 485 crore in losses. This edition asks the people running these institutions what they are doing about it and whether it is enough.

Fraud, AI and the co-operative banking imperative

Having spent more than two decades in co-operative banking, **Avinash Alandkar, CEO, Laxmi Urban Co-operative Bank Pvt. Ltd.** revealed how he has seen the sector evolve from handwritten passbook entries and paper ledgers to UPI transactions, digital KYC, and mobile banking. The pace of transformation has been extraordinary. Yet no change has required more immediate attention from banking leaders than the challenge we face today: balancing AI-driven fraud prevention with the operational realities of cooperative banks.

The infrastructure reality: Let's be honest about where we stand

When experts discuss real-time fraud detection operating at millisecond speed, they are describing systems that large private banks and FinTech firms have invested years and substantial capital in building. For a co-operative bank operating six or seven branches across semi-urban and rural regions like Latur district, that is not the starting point. Pretending otherwise serves no one.

What is realistic and what many of us are actively pursuing is a phased, partnership-led approach. Instead of building proprietary fraud detection systems from the ground up, co-operative banks can leverage shared infrastructure through NPCI platforms, RBI-regulated third-party providers, and CBS vendors that are increasingly integrating AI-based anomaly detection into their solutions. The technology does not necessarily need to reside on our own servers; it simply needs to protect our customers effectively.

In fact, co-operative banks possess a distinct advantage that larger institutions often lack which is deep

“Continuous system upgrades and coordination with payment networks are key to keeping pace with evolving threats

Ramlal Damodar Sanap
CEO, The Nashik District Urban Co-operative Banks Association Ltd.

customer familiarity. A transaction pattern that appears ordinary in a metropolitan dataset can stand out immediately when we understand a customer's business cycle, financial habits, and local context. That local intelligence, combined with capable third-party tools, can produce a far more precise fraud signal than many purely algorithmic systems. For co-operative banks, millisecond fraud detection will likely emerge through shared frameworks and federated services, and our sector must collectively advocate for affordable access to such infrastructure.

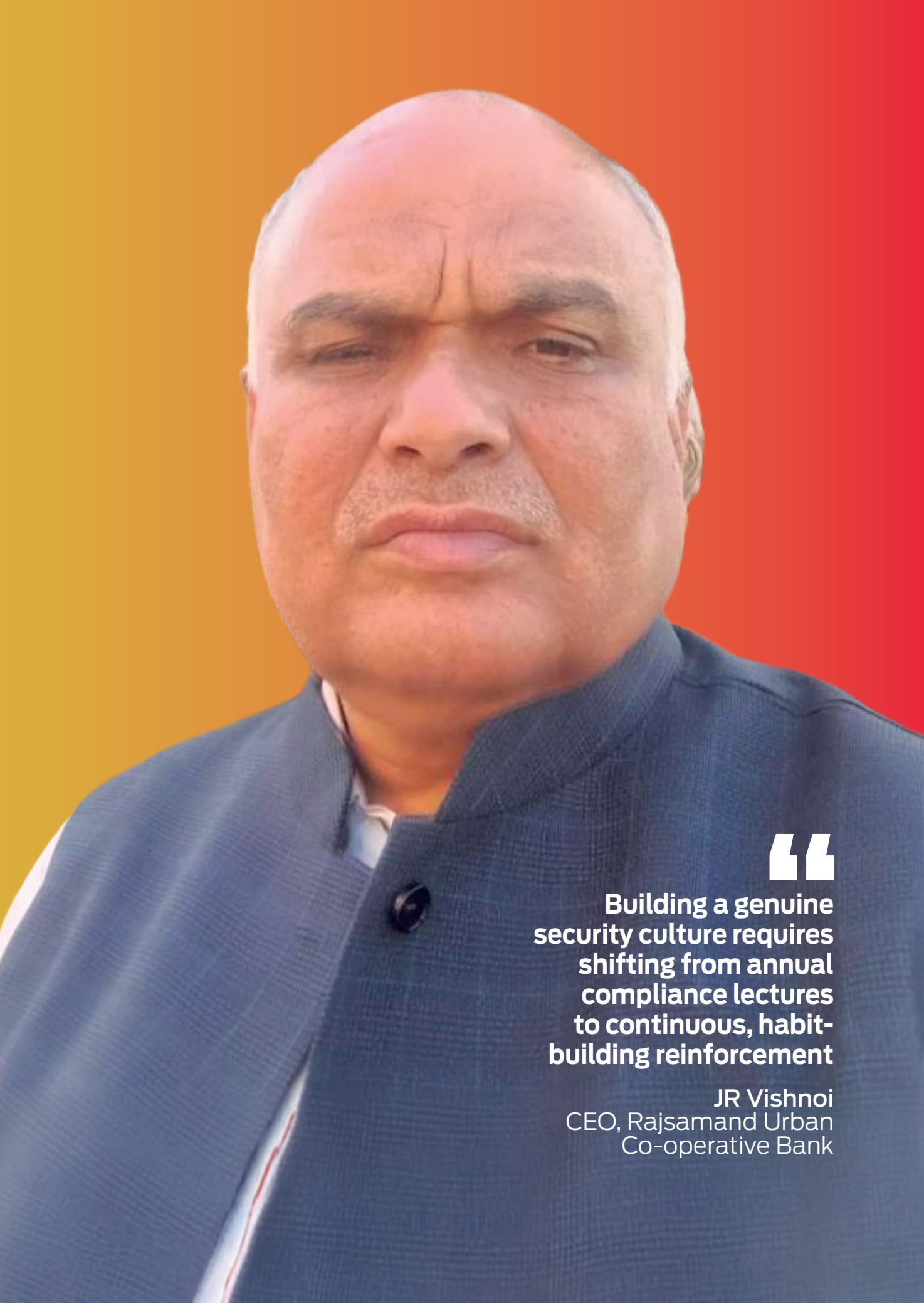
Data privacy and fraud models: Getting the balance right

The Digital Personal Data Protection Act has fundamentally reshaped how banks approach customer information. At Laxmi Urban Co-operative Bank, we have reassessed our data practices not only because regulations require it, but because customer trust is the foundation on which our institution is built.

The balance between developing effective fraud models and protecting customer privacy is complex. Our approach has been to rely on anonymised and aggregated transaction data wherever possible, while remaining transparent with customers about how their information helps safeguard their own finances. When explained clearly, most customers are not merely accepting of this approach they genuinely appreciate it. For co-operative banks, one of the most practical paths forward lies in participating in industry-level data-sharing consortiums under RBI oversight, where fraud indicators can be shared securely without exposing individual customer records. This is an area where both the RBI and IBA need to create stronger enabling frameworks for our sector.

The CBS integration bottleneck nobody talks about

There is another issue that deserves far more attention at industry forums: many co-operative banks continue



Building a genuine security culture requires shifting from annual compliance lectures to continuous, habit-building reinforcement

JR Vishnoi
CEO, Rajsamand Urban Co-operative Bank

A strong security culture requires ongoing employee training, customer awareness campaigns, phishing simulations, and leadership-driven accountability. Security must become part of daily operations rather than a one-time or annual activity

to operate on core banking systems implemented a decade or more ago. Integrating modern AI-driven fraud monitoring into these systems is rarely straightforward. It requires API compatibility, middleware support, and often difficult negotiations with CBS vendors that have traditionally prioritised larger banking institutions.

This is a genuine operational bottleneck. My advice to co-operative banking leaders is simple: challenge your CBS vendors during renewals and upgrade discussions. Ask direct questions about their AI integration roadmap. Demand service-level commitments around fraud module enhancements. The leverage exists particularly as regulatory expectations around fraud prevention continue to tighten across the sector.

At our bank, we have adopted a gradual approach, beginning with rule-based alert systems that flag unusual transaction behaviour, while building a roadmap toward machine learning capabilities as our CBS infrastructure evolves. The key is not to let the pursuit of perfection delay meaningful progress.

UPI and the expanding attack surface

UPI has transformed financial inclusion in India. At the same time, it has dramatically expanded the fraud risk landscape. The scale of digital transactions now processed by co-operative banks would have been unimaginable a decade ago, and many traditional fraud controls were simply not designed for this volume or speed.

Co-operative banks must treat UPI fraud as a distinct category of risk rather than an extension of conventional fraud management. This requires dedicated transaction monitoring, customer-facing safeguards for high-risk transfers to new beneficiaries, enhanced authentication for dormant accounts that suddenly become active, and active engagement with NPCI's fraud reporting systems.

At our bank, we have also implemented cooling periods for first-time high-value beneficiaries. While occasionally inconvenient for customers, these measures have successfully prevented genuine financial losses.

Building a genuine security culture, not a compliance exercise

Annual awareness programmes alone are not enough. A once-a-year presentation on phishing or OTP safety does not create a security culture any more than a single fire drill prepares people for a real emergency.

The human element whether it is an employee clicking on a suspicious link or a customer sharing an OTP under pressure is not something to be dismissed as carelessness. It is fundamentally a training and

communication challenge, and leadership must take ownership of it.

At Laxmi Urban Co-operative Bank, we have shifted to quarterly, scenario-based training sessions for staff, including tabletop exercises focused on fraud patterns relevant to our region. Whenever a new fraud trend emerges whether it is a UPI spoofing scam or fake government scheme calls, we brief branch teams within 48 hours and issue customer alerts in Marathi using clear, actionable language.

This approach works because cooperative banks operate on trust. Our customers already see us as local institutions that understand their realities. When we warn them about a scam, they listen. That level of community connection is difficult for larger banks to replicate. Co-operative banks may never match large private institutions in technology spending. But we can differentiate ourselves through trust, customer understanding, and community service. The path to AI-driven fraud resilience for our sector lies in honest self-assessment, strategic partnerships, continuous staff training, constructive regulatory engagement, and above all, an unwavering commitment to the people we serve every day.

Milliseconds are the new margin

Real-time fraud detection requires a combination of cloud computing, real-time data streaming, AI/ML-based risk engines, and API-driven architecture for millisecond decision-making. For co-operative banks, **Ramlal Damodar Sanap, CEO, The Nashik District Urban Co-operative Banks Association Ltd.** believed that building this fully in-house may be costly, but it is realistic through FinTech partnerships and SaaS-based solutions.

DPDP, consent and the data tightrope banks must walk

Banks must adopt a consent-driven approach, collect only necessary data, and implement strong data governance, encryption, and anonymisation. A balanced framework ensures effective fraud detection while fully complying with legal and privacy obligations.

Modernise without chaos

Integration is challenging due to outdated systems but can be managed through middleware and API layers. A phased and modular approach allows banks to add modern fraud detection capabilities without replacing the entire core system.

The payment boom nobody prepared for

Banks are strengthening controls through AI-based transaction monitoring, behavioural analytics, device fingerprinting, velocity checks, and real-time alerts. Continuous system upgrades and coordination with payment networks are key to keeping pace with evolving threats.

Culture beats compliance every single time

A strong security culture requires ongoing employee training, customer awareness campaigns, phishing simulations, and leadership-driven accountability. Security must become part of daily operations rather than a one-time or annual activity.

Speed is the only fraud strategy that works

Talking about the fraud detection strategy, **JR Vishnoi, CEO, Rajsamand Urban Co-operative Bank** spoke about how real-time fraud detection requires event-driven streaming architectures, in-memory data grids, and millisecond-latency APIs connected to AI/Machine Learning (ML) engines. It is rarely realistic for smaller co-operative banks to build this from scratch due to prohibitive costs and talent requirements. Instead, they must rely on white-labelled solutions.

The DPDPA permits processing personal data without explicit consent if it is legally required for law enforcement, regulatory compliance, or fraud detection. Because the RBI actively mandates banks to maintain robust fraud detection infrastructure and report suspicious transactions, banks use this mandate to train their models without running afoul of the Act's broader consent requirements

Good data hygiene is good fraud defence

The DPDPA permits processing personal data without explicit consent if it is legally required for law enforcement, regulatory compliance, or fraud detection. Because the RBI actively mandates banks to maintain robust fraud detection infrastructure

and report suspicious transactions, banks use this mandate to train their models without running afoul of the Act's broader consent requirements.

The legacy problem sitting at the heart of every co-operative bank

Integrating modern AI with legacy CBS platforms is highly complex. Built decades ago on monolithic structures, legacy cores rely on batch processing rather than the real-time, event-driven data flows that AI requires. For co-operative banks, this means bridging an immense architectural divide to achieve seamless AI fraud prevention.

Every new payment channel is a new attack surface

Co-operative banks adapt to this expanded transaction surface through several specific measures:

- AI/ML Fraud Monitoring: Utilising shared solutions to analyse transaction behaviour in real-time, instantly decline suspicious transfers, and flag anomalies based on spending patterns.
- Multi-Factor Authentication (MFA): Implementing stringent RBI Guidelines on Cyber security for Urban Co-operative Banks to mandate Additional Factor of Authentication (AFA) and device binding.
- Real-Time Alerts & 24x7 Helpdesks: Sending instant SMS/email alerts for electronic transactions and providing uninterrupted channels for customers to instantly report fraud.
- Shared Technology Infrastructure: Leveraging shared service entities like Sahakar Sarathi and platforms such as Sahakar DigiPay to equip smaller banks with robust, centralised fraud risk control systems.

People are the weakest password

Building a genuine security culture requires shifting from annual compliance lectures to continuous, habit-building reinforcement. This involves moving to micro-learning, designing role-specific training at the point of risk, and implementing positive recognition rather than a punishment-based approach.

The banking philosophy that puts dreams before transactions

Ashok Kumar Tiwari, CISO & DPO, Vasai Vikas Sahakari Bank (VVSB), tells **Aishwarya Saxena** why going digital never meant leaving their customers behind

The co-operative banking model is fundamentally built on trust, customer ownership, and localized decision-making. How do you ensure that this human-centric approach does not get diluted as you scale digital operations?

At VVSB, we see technology as a tool to deepen human connections, not replace them. Our customers are not just customers; they are owners. So, when we scale digital operations, we design every channel to reflect that co-operative soul. We keep it simple: our mobile app offers simple, easy-to-use features with uncluttered interfaces, and we never push a product without clear, human-understandable terms.

My role as CISO & DPO ensures the trust our customers place in us is never compromised. We use data only to understand their real needs and then the branch manager who knows them personally is still just a call or visit away. Digital tools handle routine transactions; our people handle dreams. That is how the human-centric approach scales without dilution.

Digital transformation in co-operative banks often faces legacy infrastructure constraints. What were the biggest technological bottlenecks you encountered, and how did you overcome them?

Our biggest bottleneck was our legacy core banking system and payment switch robust and reliable, but never designed for today's new technology, APIs, and real-time demands. We were

facing frequent digital transaction declines, which directly hampered our customer service. Integrating a modern mobile banking front-end with that backbone was a significant challenge. Beyond that, the bank needed to adopt entirely new technology, implement fresh features, and integrate APIs as per evolving business requirements all without disrupting day-to-day trust.

We overcame this with a carefully phased and respectful approach. Data migration was executed in verified blocks over weekends, with full backups and zero tolerance for any data loss my IT, IS, and GRC team personally oversaw every bit of that process.

The complexity intensified because we were migrating two systems simultaneously - the CBS and our entire payment switch. This was very risky, but we planned every module and activity against strict timelines and defined clear roles for every bank officer and vendor involved. The bank also appointed a cybersecurity and compliance expert consultant specifically for this project, to assess everything for a smooth, compliant migration and to report periodically to the IT Committee and the Board.

We placed heavy emphasis on staff training, thorough documentation, and rigorous User Acceptance Testing (UAT) before any go-live date. Our phased rollout plan-built confidence step by step. We started with day-to-day banking operations, then embedded system controls to meet all regulatory requirements. Next came daily MIS reporting, followed by system-generated RBI mandated reports, regulatory returns, and then customised management reports. Only after that did we activate compliance monitoring modules.

To leave no room for risk, we engaged an external agency for both pre-migration and post-migration audits. After the completion of the third phase of work in the new system, the bank conducted a full suite of audits EDP audit, IS audit, SAR, VAPT, and Cybersecurity gap assessment. This ensured we could identify and mitigate any operational or regulatory risks before they could impact our customers.

Finally, after a stabilisation period, we submitted a formal sign-off report

“We are piloting an AI-based Enterprise Fraud Risk Management (EFRM) early-warning system for all digital transactions

to the bank's Board. Throughout the entire journey, our respective executives, HODs, branch managers, and frontline bank staff worked in close coordination to verify every control on the new CBS ensuring we could deliver the best possible service to our customers. At all times, our respected Chairman, Vice Chairman, IT Committee Chairman, CEO, and the entire Board maintained direct oversight. That governance gave us the confidence to manage the risk. By keeping security, simplicity, and systematic execution at the center, we now have a platform that is modern on the outside, rock-solid on the inside, and fully trusted by everyone who operates it.

With customers increasingly expecting seamless, app-first banking experiences, how do you ensure that your strategic roadmap balances branch-led trust with digital-first convenience?

Our roadmap runs on a simple philosophy: branches build trust, digital delivers convenience two wheels of the same bicycle. For everyday needs, we have packed the VVSB Mobi Fast app with everything a customer requires without stepping out of their shop or home. They can view account balances and statements, control their ATM card instantly (Card ON/OFF, set limits for ATM, POS, e commerce, and IMPS mobile app transactions), and access UPI and IMPS for real-time fund transfers. Login is made both secure and effortless with multiple options easy PIN, biometric, face ID, or password. Customers can also open or close Fixed Deposits and Recurring Deposits digitally, view loan and FD details, download an e passbook, email statements, and even report a fraud transaction or file a complaint directly through the app.

All this self-service power sits on the digital side. But the moment a customer needs a large loan, personalised investment advice, or simply wants to talk to someone they know, the branch is still the trust anchor. So, routine transactions happen on the phone; major financial decisions still involve a human

conversation. That is how we balance app-first speed with the cooperative warmth our customers own.

FinTech companies are doing things that cooperative banks used to do like small loans, savings products, community finance. Do you see them as competition, as partners, or as a signal that the cooperative model needs to change?

FinTechs are both a wake-up call and an opportunity. Yes, they have shown that small loans can be approved in minutes with clever use of data, and that community finance can now happen on an app. That is competition we respect. But they often lack the local trust, the physical presence, and the deep, generational understanding of a customer's life that a cooperative bank has built over decades. You simply cannot code empathy.

Rather than compete head-on, we choose to collaborate. We are actively exploring partnerships where fintech firms provide sharp credit scoring models and agile technology, and we provide our trusted customer base and the last-mile relationship.

As CISO & DPO, I ensure that any such partnership puts customer data sovereignty first data stays firmly under our control, used only for customer benefit. This is not a signal that the cooperative model must change its soul; it is a signal that we must upgrade our tools. The future is a "coop-fintech" model where technology empowers, but customers remain owners, not just data points.

What emerging technologies like AI, machine learning, or blockchain do you see having practical applications within VVSB in the near future?

We are pragmatists, not dreamers. For us, AI and machine learning have immediate practical use in financial inclusion and security. We are piloting an AI-based Enterprise Fraud Risk Management (EFRM) early-warning system for all digital transactions. This system analyses transaction patterns, customer behaviour, geo-locations, and usage patterns to spot anything unusual in real time. It helps us protect customers' money before fraud happens, not after.

> **"By keeping security, simplicity, and systematic execution at the center, we now have a platform that is modern on the outside, rock-solid on the inside, and fully trusted by everyone who operates it**

Blockchain holds promise in creating transparent, tamper-proof records for customer share capital and co-operative lending groups, making settlement between co-operative banks faster and fraud resistant.

Any technology we adopt must pass a simple test does it make a customer's life easier while keeping their data private? As CISO & DPO, I sit at that intersection, ensuring every algorithm is explainable, fair, and respectful of privacy. We will never use AI to replace human judgement. We will use it, so our people spend less time on paperwork and more time with the customers who own this bank.

editor@thefoundermedia.com

Trust comes before speed when a co-operative bank goes digital

Arti Dhole, Jt. MD, Cosmos Co-operative Bank Ltd., shares with **Aishwarya Saxena** how the bank has quietly built a digital infrastructure that serves customers who are not yet ready to leave the branch behind

What does digital transformation mean differently for a co-operative bank versus a private sector bank of similar size, and how does your Bank measure the success of its digital transformation initiatives?

For a co-operative bank, digital transformation is not only about adopting technology; it is about making banking more accessible, trusted, and inclusive without losing the human connection that customers value. A private sector bank may view digital transformation largely through the lens of scale, speed, and cost optimisation. In the co-operative banking space, however, the approach has to be more balanced. We serve customers across urban, semi-urban, and community-based ecosystems where relationships still matter deeply. Customer expectations from co-operative banks are also different from those of private banks, as the customer profile itself varies significantly.

For us, digital transformation means using technology to simplify banking while preserving trust and personal engagement. The objective is not to replace people with technology, but to empower both customers and employees through technology, while also improving efficiency, automation, and cost optimisation wherever possible.

In fact, our bank implemented a modular Core Banking System as early as the 2000s, which itself required


“
Our long-term vision is to build a digitally confident banking ecosystem where technology innovation and cyber resilience evolve together in a balanced and responsible manner

significant foresight and vision at that time. Even then, the focus was not merely on digitising operations, but on enhancing customer experience and building a stronger foundation for future-ready banking services.

Over the last few years, our bank has undertaken several strategic initiatives in this direction. These include a Core Banking upgrade, a new Mobile Banking platform, WhatsApp Banking and UPI enhancements, implementation of a Loan Origination System (LOS), Fraud Risk Management solutions, data visualisation-based enterprise dashboards, passbook kiosks, and regulatory reporting automation. Each initiative has been aligned not only with operational efficiency, but also with customer convenience, service quality, governance, and regulatory readiness.

What differentiates a co-operative bank is that digital adoption levels vary significantly across customer segments and regions. Therefore, success cannot be measured only through digital transaction volumes. We evaluate a broader set of indicators such as:

- Improvement in customer onboarding turnaround time
- Increase in digital transaction adoption
- Reduction in manual processing
- Effectiveness of fraud monitoring
- Customer grievance resolution timelines
- Branch productivity
- Operational transparency
- Customer feedback across demographic segments

We also closely assess whether technology is improving service accessibility for customers who may not yet be digitally mature. In our view, a successful transformation is one where even a customer in a semi-urban branch feels more confident, secure, and empowered while banking with us.

Another important dimension is internal decision-making. With enterprise dashboards and analytics,

branch-level insights are now more data-driven and timely, enabling faster and better governance decisions.

Going forward, I believe the true success of digital transformation in co-operative banking will not be judged only by how advanced technology is, but by how responsibly and inclusively it improves the banking experience for every customer segment.

How does your bank manage cybersecurity risk across a network of 193 branches with varying levels of digital maturity?

Today, cybersecurity is no longer just an IT concern; it is fundamentally a matter of business resilience and customer trust. In banking, even a single cyber incident can impact not only systems, but also the confidence customers have built over decades. For co-operative banks especially, maintaining digital trust is absolutely critical as digital services continue to expand.

Managing cybersecurity across 193 branches with varying levels of digital maturity requires a layered and disciplined approach. Technology alone cannot solve the challenge. Cyber resilience has to be built through a combination of systems, processes, governance, and people.

Our approach begins with strengthening the core digital infrastructure. We have implemented a secured SD-WAN architecture with need-based access controls, no direct internet access for branches, and 100 per cent posture checks across branch endpoints. In addition, we have adopted a defence-in-depth approach, Zero Trust Network architecture, deception mechanisms, robust endpoint protection and detection systems, a structured review and response framework, and a Security Operations Centre (SOC). We have also enhanced monitoring systems, secured digital banking channels, and strengthened transaction surveillance mechanisms.

> **“We continuously sensitise employees about phishing risks, social engineering, cyber hygiene, password protocols, and customer data protection**

At the same time, we recognise that one of the biggest vulnerabilities in cybersecurity is human behaviour. Therefore, awareness and training play a major role in our strategy. We continuously sensitise employees about phishing risks, social engineering, cyber hygiene, password protocols, and customer data protection. Building a security-conscious culture is just as important as deploying security tools.

Governance and compliance are equally important. We align our cybersecurity practices with RBI guidelines and continuously review risk controls, access management, audit observations, and incident response mechanisms. Cybersecurity cannot remain static because threats evolve continuously. Hence, periodic reviews and upgrades are essential.

We also place significant emphasis on customer awareness. As digital adoption expands across wider demographics, educating customers about safe digital banking practices

becomes a shared responsibility. In many cases, prevention begins with awareness.

From a leadership perspective, cybersecurity must be treated as an ongoing strategic investment rather than a one-time compliance exercise. As banking becomes increasingly digital, customers will choose institutions not only for convenience, but also for security and reliability.

Our long-term vision is to build a digitally confident banking ecosystem where technology innovation and cyber resilience evolve together in a balanced and responsible manner.

With the Gram Gruh Yojana targeting rural housing, how does your bank bridge the digital divide when reaching first-time homeowners in non-urban areas?

Financial inclusion in India cannot succeed unless digital inclusion progresses alongside it. This becomes especially important in housing finance, where many first-time homeowners in rural and semi-urban areas may be entering the formal banking ecosystem for the first time.

Under initiatives such as Gram Gruh Yojana, through which we offer housing loans in Gram Panchayat and non-urban areas, our focus is not only on providing credit, but also on making the entire banking experience simple, accessible, and confidence-building for customers.

As a co-operative bank, we understand that a large section of customers and prospective customers in these regions may not always be tech-savvy or fully comfortable with digital processes, online documentation, or formal banking systems. Therefore, our approach is to combine technology with human

assistance rather than relying only on digital channels.

Technology helps us improve speed, efficiency, and transparency through systems such as the Loan Origination System (LOS), digital workflow management, and centralized processing. At the same time, our branches and field teams provide personalized support to customers at every stage — whether it is documentation, understanding eligibility, repayment planning, or digital banking usage. Personal attention is given to address customer concerns and ensure that technology does not become intimidating or difficult to use.

Relationship-based banking continues to be one of the core strengths of co-operative banks. Customers in rural and semi-urban areas often value trust, accessibility, and face-to-face guidance. Therefore, while backend processes are becoming increasingly digital, customer engagement remains highly personalized.

We are also consciously expanding user-friendly banking channels such as Mobile Banking, WhatsApp Banking, UPI services, passbook kiosks, and cash recyclers to make banking more convenient and accessible. The idea is to gradually introduce customers to digital banking through familiar and easy-to-use platforms, while also providing assistance wherever required.

Apart from housing finance, our continued focus on Self-Help Group (SHG) lending and Agri loans has also helped us deepen our presence in rural and non-urban markets. These initiatives strengthen financial inclusion while helping us stay closely connected with grassroots banking needs.

Another important aspect is financial and digital literacy. Many first-time homeowners require guidance not only in understanding loan products, but also in managing repayments, digital transactions, and banking processes. In this context,

At the same time, governance remains extremely important. Banking decisions cannot become "black box" decisions. Any AI-led framework must operate within regulatory expectations, risk controls, auditability, and fairness principles. We strongly believe that human accountability must always remain central to credit decisions

branch-level support and customer education become extremely important.

For us, inclusion is not only about reach; it is about participation with confidence. The true success of digital banking in rural India will come when customers feel that technology is helping and empowering them rather than overwhelming them.

Going forward, I believe the future of inclusive banking will depend on how effectively institutions combine digital efficiency with local understanding, trust, and human connection.

How is your Bank approaching the integration of AI and machine learning into its credit underwriting and customer service functions?

Artificial Intelligence and Machine Learning are becoming important enablers in modern banking, but their adoption must be approached responsibly and pragmatically, especially in a highly regulated environment like banking.

At our bank, we view AI not as a replacement for human judgment, but as a decision-support capability that can improve speed, consistency, risk assessment, and customer experience. In co-operative banking, relationship understanding and local knowledge continue to remain very important. Therefore, our approach is to combine data-driven intelligence with human oversight.

In credit underwriting, the objective of AI and analytics is to improve both the quality and efficiency of decision-making. Through systems such as the Loan Origination System (LOS), enterprise dashboards, and analytics tools, we are gradually moving towards more data-driven credit evaluation processes. AI and machine learning capabilities can help identify patterns, improve risk segmentation, detect anomalies, and strengthen early warning mechanisms.

This becomes particularly relevant in areas such as retail lending, portfolio monitoring, fraud detection, and turnaround time optimization. The objective is not only to make credit decisions faster, but also more informed and responsible.

At the same time, governance remains extremely important. Banking decisions cannot become "black box" decisions. Any AI-led framework must operate within regulatory expectations, risk controls, auditability, and fairness principles. We strongly believe that human accountability must always remain central to credit decisions.

On the customer service side, AI has significant potential to improve responsiveness and accessibility.

Customers today expect faster service, seamless interactions, and personalised engagement across channels. AI-enabled systems can help improve query handling, service recommendations, customer communication, and operational efficiency.

However, one important principle for us is that technology should strengthen customer relationships, not depersonalise them. We believe trust and accessibility remain core strengths of co-operative banking. Therefore, even as automation increases, maintaining empathy and human interaction remains equally important.

Going forward, I believe AI in banking will evolve from being merely a technology initiative to becoming a strategic capability. Institutions that succeed will be those that adopt AI responsibly, transparently, and with a strong focus on customer trust, governance, and long-term value creation.

What strategic thinking led the bank to conceptualise and launch youth-centric Mobile Banking application as a distinct offering?

The app was conceptualised and launched with the intention of creating a distinct banking experience specifically designed for the younger generation. The idea was to offer a banking platform that feels more relevant, intuitive, and aligned with the expectations of today's youth.

The application includes several youth-centric features focused on encouraging financial discipline and convenience, such as savings habit development tools and expense management features. It also offers 100 per cent digital onboarding through Video KYC, making the process truly paperless and seamless for customers.

Other features such as virtual debit cards, biometric login, and a modern, user-friendly interface were introduced to make banking simpler and more accessible. With biometric authentication, customers can access the app instantly without the need to remember complex passwords, creating a smoother experience.

More importantly, the app was conceptualized to ensure that younger customers feel they are interacting with a banking platform built for their generation — modern in design, easy to use, and digitally native in its overall experience.

editor@thefoundermedia.com

Dombivli Nagari Sahakari Bank bets on data discipline before AI ambition

Vishram Dixit, CEO, Dombivli Nagari Sahakari Bank tells **Aishwarya Saxena** why data discipline, not model sophistication, will define which UCBs successfully scale AI

Dombivli Nagari Sahakari Bank serves a wide band of customers ranging from large industrial clients to individual salaried borrowers and small traders. Does AI treat these as fundamentally different customer groups with separate models or is it one engine trying to serve all of them?

Most UCBs, including Dombivli Nagari Sahakari Bank (DNS), are still at an early stage of AI adoption. So, the immediate focus is not on building very advanced models. The first need is to organise data properly, improve data quality and create segment wise credit assessment frameworks. In practice, industrial clients, MSMEs, salaried borrowers and small traders behave very differently, so over time one common model will not be sufficient. A practical path for UCBs is to begin with simple scorecards for different borrower segments and then gradually move to separate risk models where scale and data permit. AI should help improve segmentation, consistency and early warning identification, but not replace branch judgment. Even basic analytics can reduce subjectivity and improve underwriting quality.

Fraud is a known risk in digital loan applications. What detection mechanisms are built into the origination pipeline and how often do they catch something real?

Co-operative banks have traditionally depended on manual vigilance, but digital lending requires layered

We are working on online account opening process with all inbuilt set up till uploading to CKYC registry

fraud controls. Dombivli Nagari Sahakari Bank is moving in a practical direction where device checks, IP checks, Aadhaar validation, financial verifications, GST verification and pattern deviation alerts can be built into the origination flow without major disruption to existing systems. Even basic document forgery checks can help prevent avoidable losses.

In the UCB segment, fraud volumes may not be very high, but the impact of even one case can be significant. So, the objective is not full automation from day one. The practical approach is progressive automation that strengthens branch controls, improves verification discipline and reduces operational risk over time.

Video KYC and Aadhaar based eKYC have different reliability profiles. Which method does Dombivli Nagari Sahakari Bank rely on more and what is the fallback when biometric verification fails?

For most UCBs, Aadhaar based eKYC remains the more scalable and dependable route because it is faster and simpler to operationalise. Video KYC is useful in selected cases, but it requires stronger process discipline, stable connectivity and trained staff. DNS Bank would therefore rely more on Aadhaar OTP based KYC as the primary channel, with Video KYC in near future. We are working on online account opening process with all inbuilt set up till uploading to CKYC registry.

Initially where biometric verification does not work, especially in the case of senior citizens or customers with worn fingerprints, branch assisted KYC remains important. Co-operative banks cannot take a purely digital approach that excludes genuine customers. The right model is a hybrid one where technology improves speed and accuracy, but accountability remains with the branch.

RBI has been tightening data governance for co-operative banks. How has that shaped what data the bank can use for AI modelling and what remains off limits?

RBI's tightening of data governance

has a direct bearing on how UCBs can adopt AI. For Dombivli Nagari Sahakari Bank, the first requirement is to ensure data localisation, purpose-based consent and controlled use of sensitive information. Most co-operative banks are still bringing together data from branches, core banking systems and digital channels, so the immediate need is data quality, standardisation and audit readiness rather than complex AI deployment.

Once data discipline is in place, AI can be used more safely for early warning signals, customer segmentation, fraud detection and operational analytics. In that sense, stronger governance is not a constraint. It is the foundation for responsible, and regulator aligned AI adoption in co-operative banks.

As Dombivli Nagari Sahakari Bank expands across states, how do multi state regulatory requirements affect AI systems and do models need recalibration for different state level lending behaviours?

The RBI, Central Co-operative Laws, State co-operative laws are supportive to the recalibration process based on state level lending behaviour.

> **Once data discipline is in place, AI can be used more safely for early warning signals, customer segmentation, fraud detection and operational analytics**

As Dombivli Nagari Sahakari Bank will grow across states, differences in customer behaviour, repayment patterns, local economic conditions and recovery timelines become more visible. Most UCBs are not yet operating fully separate state wise AI models, but a practical next step is to use analytics-based calibration. This may include comparing repayment trends across districts, adjusting thresholds and identifying local risk clusters. Over the period the multi-lingual work process with the use of AI is now possible.

Over the period, as data maturity improves, UCBs can move toward a model where central or state policy is supported by state level adjustments. That would reflect how co-operative banks already function in practice, with central/ state governance and strong local understanding. AI should strengthen this structure by improving consistency and decision support, not by replacing local knowledge.

editor@thefoundermedia.com

Shared cybersecurity is no longer optional for India's rural banking sector

B. Dinesh Kumar, General Manager, The AP State Co-operative Bank Ltd. (APCOB) speaks candidly with **Aishwarya Saxena** about the hard institutional choices that made APCOB's digital transformation both possible and sustainable

Co-operative banks compete with commercial banks, small finance banks, and FinTech platforms for the same rural customer. What unique digital value proposition can a co-operative bank offer that these competitors cannot easily replicate?

Co-operative banks have a unique digital value proposition because we combine technology with trust and local understanding. Commercial banks may bring scale, FinTechs may bring speed, and small finance banks may bring focused products, but rural co-operatives have something difficult to replicate — deep member-level and village-level context.

Through PACS, we understand the borrower beyond a credit score. We understand crop cycles, repayment behaviour, local economic conditions and livelihood patterns. Not just this, our PACS Secretary or CEO often knows about a borrower's entire family from generations. Our focus is to digitise this strength, not replace it.

At APCOB, we are exploring this through a PACS-level PoC with a third-party TSP, where PACS can function as assisted digital service points. This helps members access digital banking, payments and potentially credit facilitation through a trusted local institution.

This is important because India's digital payments ecosystem has already reached massive scale. As per NPCI, UPI recorded 22,346.80 million


Modern banking requires integrated workflows and analytics, not siloed systems with multiple vendor layers

transactions worth ₹29,02,988.05 crore in April 2026, with 712 banks live on UPI. The rural customer is also part of this digital shift, but adoption at the last mile still requires confidence and assistance.

Our USP is simple: last-mile trust delivered through modern digital systems. The future is not rural cooperatives competing with fintechs. It is co-operatives using technology to make local trust scalable.

Co-operative banks have started offering services like UPI, IMPS, NEFT, RTGS, and Positive Pay. What are the operational prerequisites a co-operative bank must fulfil before onboarding onto the NPCI-regulated payment networks?

For a rural co-operative bank, onboarding to UPI, IMPS, NEFT, RTGS or Positive Pay is not just a technology decision. It is an institutional readiness decision.

Earlier, the prerequisites were mainly CBS readiness, IFSC/ connectivity, settlement arrangements, sponsor-bank or direct membership eligibility, reconciliation processes and basic customer grievance handling. In addition, financial stability aspects such as minimum CRAR, absence of accumulated losses, controlled NPAs and satisfactory regulatory compliance record were also important.

But RBI's November 28, 2025, Directions for Rural Co-operative Banks have raised the bar. These Directions come into effect from January 1, 2026, and apply specifically to Rural Co-operative Banks. They distinguish between view-only and transactional digital banking. View-only digital banking can be launched with Board approval and intimation, but transactional digital banking requires prior RBI approval through PRAVAAH, along with CBS implementation, IPv6 readiness, CRAR compliance and a GAICA report certified by a CERT-In empanelled auditor.

In my experience, the major change is that RBI is no longer looking only at connectivity. It is looking at cyber resilience, internal controls, customer protection, data privacy, fraud risk management and continuous compliance.

So before entering NPCI/payment networks, a cooperative bank must ensure clean CBS data, secure infrastructure, liquidity and settlement discipline, strong reconciliation, transaction monitoring, trained staff, and TAT-based dispute resolution.

In simple terms, digital payment readiness is not about enabling a channel; it is about preparing the bank for real-time banking discipline.

Many co-operative banks still run on legacy or siloed IT systems. What are the key steps involved in migrating from a legacy system to a modern, cloud-ready core banking platform without disrupting day-to-day operations?

For cooperative banks, migration from legacy CBS to a modern platform should be treated as a phased institutional transition, not merely an IT change.

In APCOB's case, we were earlier operating on a licence-based, on-premises CBS model. Over time, with increasing infrastructure requirements, software upgrades, cybersecurity expectations and higher compute needs, it became difficult to sustain this model efficiently. We therefore migrated to the NABARD-promoted ASP model CBS in a phased manner — first at the StCB level and subsequently across DCCBs over two years, during 2021 and 2022.

Earlier, the StCB and DCCBs were operating on different CBS platforms.

Now, being on the same CBS has significantly improved data availability, monitoring, reporting and analytics capability across the co-operative structure.

The key steps in such migration are assessment of existing data and customisations, data cleansing, migration planning, parallel run, user acceptance testing, cybersecurity validation, DR readiness, staff training and then final cutover. For smaller RCBs, SSPL-type shared service models are the most practical way to stay updated, secure and scalable. Licence-based or on-premises models involve heavy capital cost and continuous upgrade burden, particularly in today's dynamic threat landscape.

Modern banking requires integrated workflows and analytics, not siloed systems with multiple vendor layers. Too many fragmented systems increase operational risk as well as vendor risk.

In simple terms, co-operative banks need shared, secure, integrated and data-ready platforms.

Cybersecurity is a growing concern with the expansion of digital banking. What specific cybersecurity vulnerabilities are co-operative banks most exposed to, and what frameworks would you recommend to mitigate them?

For rural co-operative banks, the main cybersecurity vulnerability is that our digital exposure is increasing faster than our individual investment capacity. Because of smaller book sizes, many RCBs cannot independently afford high-end security architecture, 24x7 monitoring, advanced SIEM tools, CSOC, endpoint detection, API security and specialised cyber manpower.

The major risks are phishing and social engineering, weak endpoint security at branches, delayed patching, vendor dependency, inadequate monitoring, ransomware, credential

compromise and gaps in incident response.

This becomes even more important now because RBI's 2025 Digital Banking Directions for Rural Co-operative Banks have made cyber resilience, internal control assessment, GAICA review by CERT-In empanelled auditors, CBS readiness and stronger technological controls central to digital channel authorisation.

In my view, the practical framework is a shared cybersecurity model. Like shared CBS or ASP platforms, co-operative banks can collectively build CSOC, SIEM, threat monitoring, vulnerability management and incident response capabilities.

Even endpoint security can be procured jointly. In practical procurement experience, collective bargaining and bulk procurement can reduce pricing significantly — in some cases by around 30–40 per cent compared to each small bank negotiating separately.

For smaller RCBs, cybersecurity cannot remain only a bank-wise burden. It must become a sector-level shared infrastructure, with bank-level responsibility for access control, staff awareness, customer education and local governance.

In simple terms, the threat is enterprise-grade; therefore, the defence also has to be ecosystem-grade.

Co-operative banks are deeply embedded in rural economies. How can digitisation help them better serve farmers, particularly through integration with government schemes like PM-KISAN, KCC or crop insurance portals?

Digitisation can help co-operative banks move from scheme delivery to timely, data- backed farmer service.

Farmers today interact with multiple systems like PM-KISAN, KCC, crop insurance, land records, dairy data and subsidy platforms. If co-operative banks can integrate these data points

into lending workflows, credit can become faster, more accurate and more contextual.

At APCOB, our first step in this direction was with RBIH on digital KCC, through the Public Tech Platform for Frictionless Credit, which has now evolved into the Unified Lending Interface, or ULI. RBIH describes ULI as a platform that enables lenders to use digital data sources within lending workflows for faster and more inclusive credit.

We also implemented digital Dairy Loan Origination System through this platform, and nearly 300 dairy loans were processed through this route. This is important because dairy income, milk pouring data and repayment capacity can be assessed more objectively.

This is where co-operative banks have a natural advantage. We are not distant lenders. Through PACS and DCCBs, we are embedded in the farmer's economic life.

For co-operative banks, the future is clear: PACS-level trust, integrated government data, and digital workflows can together create faster and more responsible farmer credit.

Many co-operative bank customers are first-generation banking users. How do you balance the push for digital channels with maintaining human touchpoints so that no customer segment is excluded?

For co-operative banks, digital inclusion cannot mean forcing every customer to become self-service overnight. Many of our members are first-generation banking users — elderly customers, small farmers, SHG members and semi-literate users. For them, trust comes before technology.

India has achieved massive formal financial inclusion. As per PMJDY data as on May 6, 2026, there are 58.15 crore Jan Dhan beneficiaries, of which 45.42 crore are in rural/semi-urban centres and 32.43 crore are women beneficiaries. These numbers show that access has expanded significantly. But the next challenge is meaningful usage. So, our approach is not digital-only but assisted digital.

> **"At APCOB, we are exploring this through a PACS-level PoC with a third-party TSP, where PACS can function as assisted digital service points**

The PACS and branch network becomes very important here. A customer may first use UPI, account services or digital loan application with help from PACS staff or branch staff. Gradually, confidence improves and some customers move to self-use. This transition is more realistic than expecting immediate independent adoption.

At APCOB, our PACS-level PoC through third-party TSPs is also in this direction — making PACS local assisted digital service points. Similarly, digital workflows like KCC or dairy LOS should not remove human support; they should make service faster while keeping explanation and guidance local.

In simple terms, technology should not replace trust; it should strengthen trust. Our objective is to make banking digital, but not impersonal.

editor@thefoundermedia.com

Why wrapping a legacy system is often wiser than replacing it

Ravikiran Mankikar, CMD, RKM Consultants explains to **Aishwarya Saxena** why moving to cloud is the easy part and proving control discipline after the move is where most banks quietly struggle

Many smaller co-operative banks still run on legacy core banking systems built in the early 2000s. Can those systems even be retrofitted to meet DPDP obligations, or is a rip-and-replace conversation unavoidable?

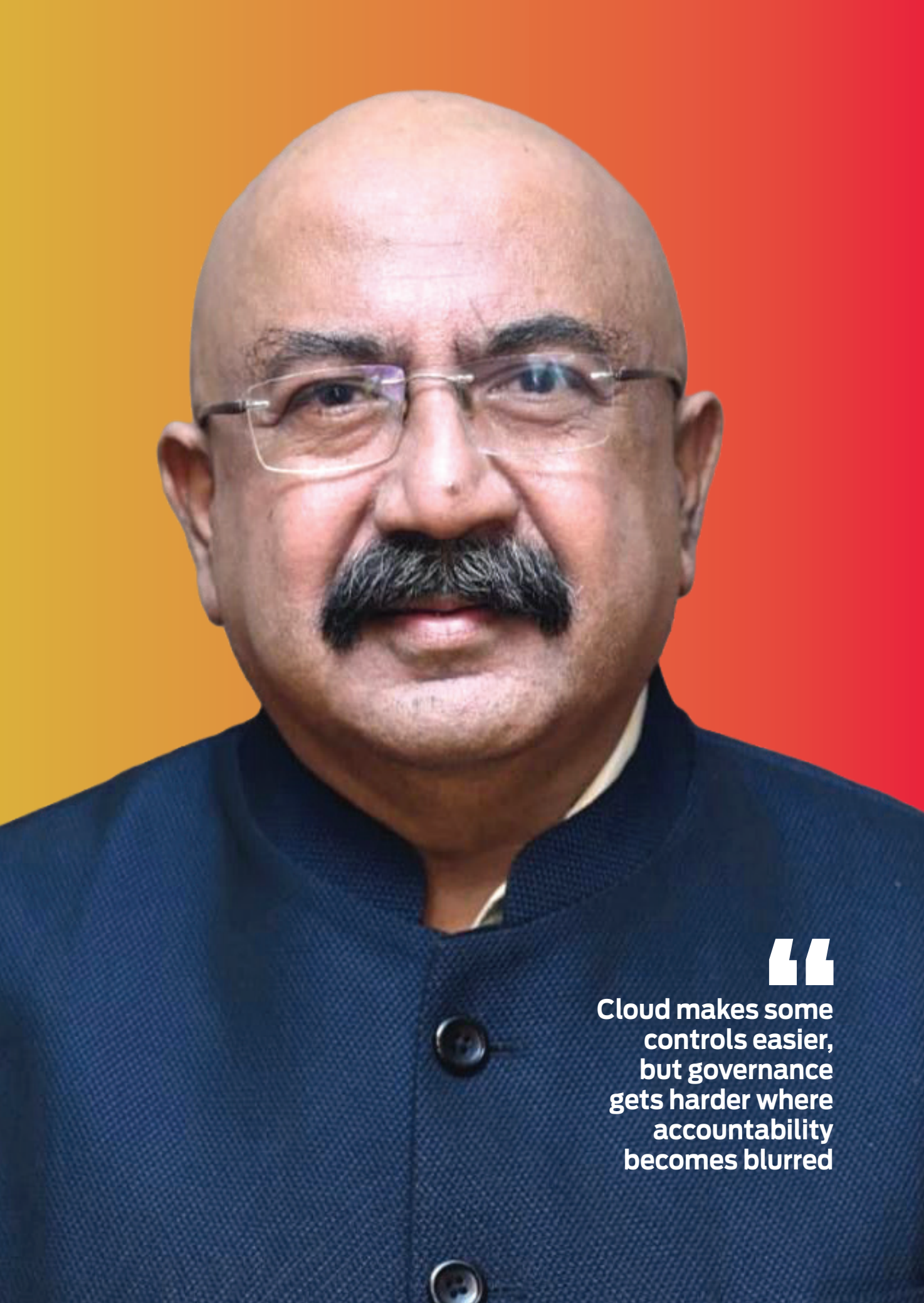
A full remove-and-replace is not automatically unavoidable. In many smaller co-operative banks, the practical path is a phased retrofit: data mapping, consent and purpose tagging, access control hardening, retention rules, audit logs, and masking/tokenisation around the core rather than immediate replacement.

The problem is that many legacy CBS platforms were not designed for privacy-by-design, so if the bank cannot reliably identify where personal data sits, who can access it, and how deletion or retention is enforced, retrofit becomes expensive and brittle.

The rule of thumb is simple: if the core can support data inventory, event logging, field-level controls, and API-based overlays, retrofit is possible; if not, replace the core in phases, starting with customer-facing and data-exposure layers.

A phased modernisation via middleware is usually the better risk-adjusted path for DPDP-driven uplift, while full remove-and-replace is justified only when the legacy core cannot support basic control evidence, data segregation, or reliable integration at all.

The matrix below compares both



“Cloud makes some controls easier, but governance gets harder where accountability becomes blurred

Criterion	Phased modernisation via middleware	Full remove and replace
DPDP consent-management fit	High, if consent capture/withdrawal is implemented in middleware or adjacent services and the core is left as a system of record.	High in principle, but only after the new platform is fully implemented and migration is clean; during transition, consent consistency can break.
Automated audit trails	High, because middleware can centralise logging, event capture, and workflow evidence without rewriting the core.	High after go-live, but migration is the hardest period for preserving uninterrupted traceability across old and new systems.
Data sovereignty controls	Medium to high, if the bank overlays location controls, encryption, tokenisation, and processor governance around the existing core.	High if designed well, but only if the target architecture, contracts, and hosting model are controlled from day one.
Legacy workflow preservation	Very high; this is the main advantage because 20-year-old branch and back-office processes can remain intact while controls are modernised.	Low to medium; workflows often need redesign, retraining, and process re-engineering, which is disruptive for smaller UCBs.
Technical feasibility	High for a large subset of compliance use cases, especially where the goal is to wrap, instrument, and govern rather than re-platform.	Medium; feasible, but execution risk is much higher because data migration and cutover complexity rise sharply.
Data loss risk	Low to medium, because the core remains operational and migration can be incremental.	Medium to high, especially during conversion, reconciliation, and cutover windows.
System failure risk	Medium, mainly from middleware misconfiguration, integration latency, or poor change control.	High, because a failed go-live can affect the entire bank's operational continuity.
Implementation timeline	About 6 to 18 months for meaningful compliance uplift, depending on scope and vendor readiness.	About 18 to 36 months for a controlled replacement in a small bank, longer if data quality is poor.
Cost profile	Lower upfront capex; costs are spread across integration, controls, licenses, and process redesign.	Much higher upfront cost due to platform, migration, testing, training, parallel runs, and cutover support.
Best use case	Banks that need fast DPDP controls without destabilising branch operations.	Banks whose legacy core is too rigid, unsupported, or impossible to secure and observe adequately.

approaches specifically on consent management, audit trails, and data sovereignty, using a practical CIO lens rather than a theoretical architecture lens.

AI-driven credit scoring and fraud detection consume enormous amounts of personal data. Under the DPDP framework, how do you govern AI systems that are making consequential decisions about individuals?

Under DPDP, the governance question is not whether AI is "smart," but whether the bank can justify data use, prove purpose limitation, and control downstream sharing. For credit scoring and fraud detection, that means explicit data governance, clean consent or other lawful basis where applicable, minimisation of inputs, model explainability, bias testing, audit trails, and human review for adverse decisions.

In practice, banks should treat AI models as regulated decision-support systems: document training data sources, define prohibited attributes and proxy variables, set approval thresholds, and maintain a model-risk committee with compliance, credit, risk, IT, and legal ownership.

If a model can materially affect access to credit, the bank should be able to explain the decision in plain language, not just produce a score.

Relying too heavily on AI decisions under the DPDP framework creates serious privacy, fairness, and accountability risks because banks may not be able to fully explain how personal data was used or why a particular outcome was produced.

In practice, this can lead to biased or discriminatory decisions, excessive data collection, and weak human oversight, especially when models are trained on large datasets without clear purpose limitation or robust governance.

RBI's guidelines on critical information systems and third-party oversight have tightened significantly. In your view, how many co-operative banks have a genuinely mature vendor risk management programme?

Honestly, the sector does not have the required maturity here; most co-operative banks are still at a compliance-checklist stage rather than a genuinely resilient third-party risk programme. RBI's approach is toward board-approved outsourcing policies, continuous monitoring, concentration-risk control, audit rights, breach response, and exit planning, which many smaller banks struggle to operationalise consistently.

The usual weakness is that contracts exist, but inventory, ongoing assurance, subcontractor visibility, service testing, and termination readiness are not truly embedded in day-to-day governance. Some banks have mature programmes, but majority have partial controls, and many still rely on trust, not evidence.

Strengthening vendor risk maturity in a co-operative bank is no longer optional because outsourced IT, cloud, payment, and fintech dependencies can create operational, cyber, and regulatory failures even when the bank's own internal controls look sound. A mature vendor risk programme means the bank does not stop at onboarding due diligence; it continuously assesses security posture, contractual safeguards, audit rights, incident reporting, data handling, and exit readiness so that third-party weakness does not become a customer-data breach or service outage.

For co-operative banks, this is especially important because limited in-house capacity often makes them more dependent on vendors for critical services, which increases concentration risk and reduces room for error. In short, vendor risk maturity protects customer trust, supports RBI-aligned governance, and turns outsourcing from a hidden vulnerability into a controlled operating model.

Cloud adoption in banking is accelerating. RBI has its own cloud guidance now. When a co-operative bank moves to cloud, where does IT governance genuinely get harder, not easier?

Cloud makes some controls easier, but governance gets harder where accountability becomes blurred. The hard parts are shared responsibility, data location and cross-border processing, identity and privileged access management, configuration drift, dependency on the provider's control plane, and proving exit readiness without operational disruption.

For a co-operative bank, cloud also increases the burden on contract management, continuous assurance, and incident coordination because the bank still owns the risk even when the infrastructure is outsourced.

In other words, cloud reduces hardware burden but increases control discipline; if the bank's governance is weak, cloud amplifies weakness faster than it fixes it.

A co-operative bank should improve cloud governance by first assigning clear ownership, defining which workloads may move to cloud, and writing board-approved policies for data classification, access control, backup, retention, and incident response. It should then create a RACI-based governance structure, enforce strong identity and privileged-access controls, monitor compliance continuously, and require vendor due diligence, audit rights, and exit planning before any migration goes

live. For banking specifically, the hardest part is not buying cloud services but maintaining evidence of control, regulatory compliance, and data-location discipline across outsourced environments.

Being in this industry for such a long time, what's the problem in India's financial sector that nobody is talking about seriously enough, and that genuinely keeps you up at night?

The biggest under-discussed problem is not technology itself; it is the institutional habit of treating compliance as a document exercise instead of an operating model.

Many financial institutions still run with fragmented data, unclear ownership, weak process discipline, and a tolerance for manual workarounds that only become visible after a breach, fraud, or inspection. That creates a silent fragility: the bank looks functional on paper, but it cannot confidently answer basic questions about data lineage, vendor exposure, model decisions, or operational exit paths.

That is what is the cause of worry, because it turns every new initiative—AI, cloud, digital lending, outsourcing—into an accumulation of hidden risk rather than a capability upgrade.

For a small co-operative bank, phased modernisation typically lands in a lower-cost band because the bank keeps the existing CBS and invests in integration, data governance, logging, consent services, and security controls around it. A realistic planning range is roughly 15 per cent to 35 per cent of the cost of a full replacement for the first wave of compliance modernisation, though the exact number depends on vendor APIs, number of branches, and how much workflow automation is added. Full changeover usually carries the highest total programme cost because the bank pays for the new platform, migration factory, dual-running, training, testing, and contingency support all at once.

> **The biggest under-discussed problem is not technology itself; it is the institutional habit of treating compliance as a document exercise instead of an operating model**

If one measures the data loss risk, phased modernisation is usually safer because it minimises large-scale migration events and preserves the existing system of record during the transition. The main risk is control inconsistency between the core and middleware layers, especially if identity, consent, and retention rules are not centrally governed.

If one measures the system failure risk, full replacement is riskier because one bad cutover can affect deposits, loans, clearing, branch operations, and reconciliations simultaneously.

editor@thefoundermedia.com

Strengthening resilience for sustainable growth in urban co-operative banks

Vivek Gupta, Joint Director, National Federation of Urban Cooperative Banks and Credit Societies Limited (NAFCUB) reminds the sector that as Urban Co-operative Banks expand their digital footprint, cyber security can no longer remain an afterthought

The Urban Co-operative Banking (UCB) sector has historically played a vital role in extending banking services to small businesses, middle-income households, self-employed individuals, traders, professionals, and underserved urban communities. The strength of Urban Co-operative Banks lies not merely in their financial position, but in their deep social connect, local understanding, and co-operative character. At a time when global financial systems are experiencing increasing uncertainty, strengthening the financial resilience of UCBs has emerged as both a regulatory priority and a strategic necessity.

Over the last few years, the Reserve Bank of India (RBI) has introduced several reforms relating to capital adequacy, governance, risk management, and supervisory framework for UCBs. The revised regulatory mechanisms and prudential norms are aimed at enhancing depositor confidence and improving the long-term sustainability of the sector. At the same time, many UCBs

Technology-based credit monitoring systems and early warning mechanisms can significantly improve asset quality and reduce future financial stress

have demonstrated improved financial indicators, including stronger capital positions and better operational resilience.

However, sustainable strengthening of the sector cannot be achieved through regulation alone. Financial resilience in UCBs must be built mainly upon these three interconnected pillars — robust capital strength, a prudent credit culture, and sound governance supported by effective crisis preparedness.

Capital strengthening: The foundation of stability

Capital remains the first line of defence for any financial institution. In the co-operative banking structure, however, capital mobilisation has traditionally been challenging due to limitations in share capital structure, co-operative ownership patterns, and restricted access to external capital markets.

Despite these structural constraints, several UCBs have improved their Capital to Risk-Weighted Assets Ratio (CRAR) through internal accruals, disciplined balance sheet growth, and better recovery management. RBI's emphasis on stronger capital adequacy norms further reinforces the need for financially sound institutions capable of absorbing financial shocks.

At the same time, capital strengthening in UCBs requires a balanced and sector-sensitive approach. Unlike commercial banks, UCBs operate on member-centric principles within localised geographies and have limited avenues for market-based capital raising. Therefore, prudential regulations must strengthen stability without undermining the cooperative character and operational viability of the sector.

There is a growing need to explore innovative and cooperative-friendly capital augmentation measures. Encouraging long-term member deposits, facilitating special share instruments within the co-operative framework, supporting consolidation of weak entities with stronger institutions, and creating enabling policy support for capital enhancement can significantly strengthen the sector.

Equally important is the need to improve profitability. Sustainable capital generation is possible only when institutions maintain healthy earnings. UCBs must therefore focus on operational efficiency, diversified income streams, cost rationalisation, and technology-driven service delivery. Investments in digital banking infrastructure, cyber security, and professional management should not be viewed as expenditure alone but as a long-term measure for protecting institutional stability and depositor confidence.

Credit discipline and asset quality

The second pillar of resilience is prudent credit management. Relationship-based banking has historically been one of the greatest strengths of the cooperative banking sector. However, in a competitive and rapidly evolving financial environment, traditional practices alone are no longer sufficient.

Financial resilience depends significantly on asset quality. Weak underwriting standards, concentration risks, inadequate monitoring, and governance-related lapses have contributed to stress in certain institutions in the past. The experience of the sector clearly demonstrates that growth without credit discipline is unsustainable.

Strengthening professional credit appraisal systems is therefore essential. Credit decisions must become increasingly data-driven, risk-sensitive, and supported by proper due diligence. Greater emphasis on borrower assessment, cash-flow analysis, sectoral evaluation, and prudent lending practices can help reduce the buildup of stressed assets.

Technology-based credit monitoring systems and early warning mechanisms can significantly improve asset quality and reduce future financial stress. Simultaneously, strong internal controls, periodic portfolio reviews, and timely corrective measures remain critical for maintaining healthy balance sheets.

RBI's revised framework providing greater operational flexibility to UCBs in areas such as housing finance and small-value lending presents significant growth opportunities. However, such opportunities must be accompanied by robust risk governance and portfolio diversification. Excessive exposure to sensitive sectors should be avoided.

Recovery mechanisms also require continuous strengthening. A culture of timely repayment and responsible borrowing is essential for the sustainability of co-operative banking institutions. Effective follow-up systems, member engagement, legal recovery support, and settlement mechanisms can improve recovery performance while preserving co-operative values.

Another important area is human resource development. Many UCBs, particularly smaller institutions, require continuous training in credit appraisal, treasury operations, compliance management, cyber security, and risk management. Capacity-building initiatives and knowledge-sharing programmes therefore assume considerable importance in strengthening institutional resilience.

In this context, Mission SAKSHAM (Sahkari Bank Kshamta Nirman), launched by the RBI in April 2026, will prove be an important initiative for strengthening skill development and professional training in the co-operative banking sector, with the objective of enhancing systemic stability and supporting the sector's long-term sustainable growth.

Governance and crisis preparedness

Financial stress in co-operative banks

often arises not only from financial weakness but also from governance deficiencies. Weak internal controls, delayed decision-making, lack of professional expertise, and inadequate oversight can quickly erode depositor confidence.

In today's environment, trust remains the most valuable asset for cooperative banks. RBI has repeatedly emphasised the importance of operational resilience, regulatory compliance, and protection against cyber and technology-related risks. Crisis management, therefore, cannot remain reactive. Every UCB should develop a clearly defined crisis response framework covering liquidity stress, cyber incidents, operational disruptions, fraud management, and reputational risks.

Liquidity management deserves special attention. Sudden withdrawal pressures can destabilise even fundamentally viable institutions. Maintaining adequate liquidity buffers, diversified funding sources, and sound treasury management practices is therefore essential.

Cyber security has also emerged as a major area of concern. As UCBs expand digital banking services, they simultaneously become more vulnerable to cyber threats. Investments in secure digital infrastructure, regular system audits, employee awareness programmes, and real-time monitoring systems are no longer optional requirements.

Governance reforms must also focus on professionalism in board functioning. Directors and senior management should possess adequate banking knowledge, regulatory understanding, and risk awareness. Co-operative principles and professional banking standards must complement each other for the sector to remain stable and credible. There is increasing recognition that strong governance standards, transparency, accountability, and effective crisis preparedness are essential for the long-term sustainability of UCBs.

The way forward

Urban Co-operative Banks continue to occupy an important position in India's financial ecosystem by serving small businesses, traders, self-employed individuals, middle-income households, and local communities. Their relevance is expected to grow further as the country moves toward the broader national objective of Viksit Bharat @ 2047.

The co-operative banking structure remains closely aligned with the philosophy of "Sahakar Se Samriddhi" — prosperity through cooperation. The strength of UCBs lies in their local connect, community participation, and relationship-based banking model. Preserving these co-operative values while adapting to modern banking practices will be essential for long-term sustainability.

The future growth of UCBs must therefore be built upon stronger capital foundations, prudent credit culture, professional governance standards, and robust crisis management systems. Institutions must focus on improving operational efficiency, strengthening internal controls, enhancing risk management practices, and maintaining depositor confidence through transparency and accountability.

Technology and Artificial Intelligence (AI) are also expected to play an increasingly important role in the transformation of the sector. AI-based systems can support early detection of financial stress, fraud monitoring, compliance management, cyber security surveillance, and data-driven decision-making. Digital banking expansion, combined with responsible adoption of AI and modern technology, can help UCBs improve efficiency, strengthen resilience, and expand outreach among younger and technology-oriented customers.

At the same time, technological advancement must remain balanced with human oversight, ethical practices, and customer trust. The co-operative banking model has always been built upon credibility, personal relationships, and community confidence. Technology should strengthen these values rather than replace them.

The RBI's SAKSHAM initiative is also expected to play an important role in enhancing capabilities, strengthening resilience and supporting sustainable growth in UCBs. NAFCUB is also conducting specialised training programmes and workshops for boards of directors and senior functionaries to strengthen professional management, promote a strong compliance culture, encourage ethical banking practices, and enhance institutional transparency and accountability.

> **"Co-operative principles and professional banking standards must complement each other for the sector to remain stable and credible**

The path ahead requires coordinated efforts from regulators, policymakers, federations, boards of management, and banking professionals to ensure that the sector evolves in a stable and sustainable manner. With timely reforms, responsible governance, technological modernisation, and continued commitment to co-operative principles, Urban Co-operative Banks can emerge as stronger institutions contributing significantly to financial inclusion, local economic development, and the broader vision of a resilient and inclusive Viksit Bharat @ 2047 guided by the spirit of "Sahakar se Samriddhi".

Co-operative banking in a UPI-first economy: Adapting or being left behind?

Ravindra Misra, Chief Product Officer, OPL, emphasises that the future of co-operative banking will not be defined by who adopted UPI first, but by who built the smartest financial services on top of it

India's payments story has been decisively rewritten by UPI. What began as a convenient transaction layer has become the country's most visible banking interface- used daily by households, merchants, MSMEs, and institutions across urban and rural India. Inevitably, this transformation raises a critical question for India's co-operative banks: are they adapting to a UPI-first economy, or risk being left behind? The honest answer is more nuanced than a simple yes or no. Co-operative Banks are adapting- and in meaningful ways. But adaptation alone is not enough. The real challenge now is conversion: transforming UPI participation into sustainable growth, relevance, and intelligence.

Signs of adaptation: The co-operative sector is moving

There is growing evidence that the co-operative banking ecosystem is not standing still. At a national level, institutions and policymakers are actively pushing digitalisation. The National Urban Cooperative Finance and Development Corporation (NUCFDC) has taken significant steps to bring urban cooperative banks into the digital mainstream. Its 2025 initiative, Sahakar DigiPay, was designed to connect UCBs more deeply with the UPI network, enabling secure digital transactions while maintaining regulatory oversight. For a sector long constrained by legacy systems, this was a meaningful step forward.

UPI participation without intelligence turns co-operative banks into silent utilities while faster, tech-driven players capture value by building services on top of those transactions

Similarly, NABARD's push to digitalise cooperative banks by 2025 brought in a broader, structural shift- the focus of which was beyond payments enablement. It also concentrated on modern banking services-core system upgrades, interoperability, and readiness for digital products that customers increasingly expect.

Where the gap remains: Adoption without intelligence

And yet, from a product and technology standpoint, a crucial gap persists. Many co-operative banks today are UPI-enabled, but not UPI-aware.

Transactions flow smoothly. QR codes are widely accepted. Customers use UPI daily. But the data generated by this activity- transaction frequency, merchant collections, and cash flow patterns often remain disconnected from lending, risk assessment, and product innovation.

Entities like Airtel Payments Bank, and IPPB (India Post Payments Bank) are aggressively targeting the same rural and semi-urban customer base that cooperative banks serve but with superior digital interfaces and UPI integration.

This is where the risk of being "left behind" quietly creeps in. In a UPI-first economy, relevance is no longer defined by branch presence or account ownership. It is defined by who understands the customer best and acts in real time.

UPI participation without intelligence turns cooperative banks into silent utilities while faster, tech-driven players capture value by building services on top of those transactions.

From payments to possibilities: The next phase of adaptation

The next phase of adaptation for cooperative banks lies in turning UPI data into lending intelligence. From the lens of digital lending infrastructure, UPI transactions offer something co-operative banks have historically lacked access to

at scale: live behavioural signals. A merchant's daily QR collections, inflows and outflows, seasonality, and transaction regularity often reveal more about creditworthiness than static paperwork.

When combined with AI-driven underwriting and policy-based decisioning, this data can enable:

- Prequalified working capital for MSMEs
- Short tenure loans aligned to real cash-flow cycles
- Micro-credit for thin-file or first-time borrowers

Crucially, this does not mean abandoning prudence. It means augmenting traditional risk frameworks with real-world signals, something cooperative banks are uniquely positioned to do, given their deep community relationships.

Credit at the point of need without losing discipline

UPI has changed not just how people pay but also when they expect support. Customers increasingly seek credit at the point of need- embedded, contextual, and frictionless. This opens the door for transaction-triggered and QR-linked credit journeys, where offers are generated based on behaviour and routed through controlled, auditable decision engines.

Done correctly, these approaches allow co-operative banks to match FinTech-level speed without compromising regulatory discipline or governance. The key enabler here is infrastructure: end-to-end digital loan journeys, seamless CBS integration, built-in compliance checks, and scalable systems designed for high-volume, small-ticket lending.

So, are co-operative banks being left behind? Not quite. But they are at an inflection point. Co-operative banks have adapted to UPI as a payments ecosystem. The next and decisive step is adapting to UPI as a strategic platform. Those that connect payments with credit, intelligence, and compliance will remain central to India's financial future. Those that stop at enablement risk becoming invisible in a landscape where customer engagement happens every day, on a mobile screen. Co-operative banks hold decades of transactional and behavioural data on local communities, yet they are missing the analytics infrastructure to monetise or leverage this data for credit underwriting, product personalisation, or fraud detection. In a UPI-first economy where data is currency, the use of such data can be a significant opportunity for co-operative banks.

> **The next phase of adaptation for co-operative banks lies in turning UPI data into lending intelligence**

Connecting smarter in a UPI-first India

In a UPI-first economy, co-operative banks do not need to compete louder or faster; they need to connect smarter. They already have trust, reach, and relevance at the grassroots. With the right digital and AI-driven infrastructure, they can convert those strengths into sustainable growth.

The future of co-operative banking will not be defined by whether banks adopted UPI, but by what they chose to build on top of it.

AI adoption in urban co-operative banks

Dr. Anupam Gupta, Co-Founder and Director, Bharat Network Group (BNG), highlights AI's growing role in helping Urban Co-operative Banks compete smarter while keeping human relationships at the centre

Balancing technology with trust

The Indian banking sector is rapidly evolving with digital transformation, automation, and customer-centric innovation. While private and public sector banks have aggressively adopted new technologies, Urban Co-operative Banks (UCBs) are also steadily modernising their operations to remain competitive and relevant. Among the most impactful technologies driving this transformation is Artificial Intelligence (AI).

Urban Co-operative Banks have traditionally been known for their personalised service, community trust, and relationship-driven banking. However, changing customer expectations, increasing cybersecurity risks, and rising regulatory requirements are encouraging co-operative banks to adopt smarter and more efficient systems.

Today's customers expect banking services that are fast, secure, digital, and available anytime. AI is helping banks meet these expectations while improving operational efficiency and customer experience.

Why AI matters for UCBs

Urban Co-operative Banks face several challenges, including:

- Increasing competition from private banks and FinTech companies
- Manual operational processes
- Rising compliance requirements
- Growing cyber fraud risks
- Pressure to improve customer experience

AI helps address these challenges by automating routine tasks, analysing data, improving security, and enabling faster decision-making.

AI in customer service

One of the most visible applications of AI is customer support through chatbots and virtual assistants. These systems can instantly respond to customer queries related to:

“AI-powered systems can monitor transactions in real time and identify suspicious activities immediately

- Account balances
- Loan enquiries
- EMI details
- Deposit schemes
- Transaction history

This improves customer convenience while reducing workload on branch staff.

Several Urban Co-operative Banks have already strengthened their digital infrastructure. Saraswat Co-operative Bank has enhanced its digital banking ecosystem through internet and mobile banking services, while Cosmos Co-operative Bank has invested significantly in technology modernisation to improve customer accessibility and operational efficiency.

Such initiatives create a strong foundation for future AI-driven banking services.

AI for fraud detection and security

As digital banking transactions increase, cybersecurity has become a major priority for banks.

AI-powered systems can monitor transactions in real time and identify suspicious activities immediately. These systems continuously learn from customer behaviour patterns and improve fraud detection capabilities over time.

Following previous cybersecurity challenges, Cosmos Co-operative Bank strengthened its digital security infrastructure, highlighting the importance of intelligent monitoring systems in co-operative banking.

AI can help Urban Co-operative Banks:

- Detect unusual transactions
- Prevent fraud attempts
- Strengthen cybersecurity
- Improve customer trust

Faster Loan Processing

Loan processing in many co-operative banks still involves manual verification and lengthy documentation. AI can simplify this process by automating:

- Document verification
- Credit assessment
- Risk evaluation

This reduces turnaround time and improves customer satisfaction.

NKGSB Co-operative Bank and Janata Sahakari Bank, Pune have focused on improving digital banking capabilities, helping enhance operational efficiency and customer services.

AI-based lending systems can further help co-operative banks provide faster credit support to retail and MSME customers.

Personalised banking experience

AI-powered analytics helps banks better understand customer preferences and financial behaviour. Based on this analysis, banks can offer:

- Customised loan products
- Personalised deposit schemes
- Targeted financial services

Urban Co-operative Banks already have strong local customer relationships. AI can help them use customer insights more effectively to improve engagement and retention.

AI in Compliance and Operations

AI can also support banks in compliance and governance by automating:

- KYC verification
- AML monitoring
- Regulatory reporting
- Audit tracking

This reduces manual errors and improves operational transparency.

Banks like Bassein Catholic Cooperative Bank and Thane Bharat Sahakari Bank have invested in digital process improvements, reflecting the growing importance of technology in co-operative banking operations.

Challenges in AI adoption

Despite its benefits, UCBs still face certain challenges:

- Limited IT infrastructure
- Budget constraints
- Lack of skilled manpower
- Data privacy concerns

> **“The biggest strength of Urban Co-operative Banks has always been trust and personal relationships**

However, cloud-based solutions and FinTech partnerships are making advanced technologies more affordable and accessible for co-operative banks.

Technology with human trust

The biggest strength of Urban Co-operative Banks has always been trust and personal relationships. AI should support employees, not replace them.

The ideal future lies in combining:

- Intelligent technology
- Human relationships
- Community-focused banking

Banks that successfully balance technology with trust will emerge stronger and more competitive in the future.

Conclusion

Artificial Intelligence is becoming an important growth driver for Urban Co-operative Banks. By adopting AI strategically, cooperative banks can modernize operations, strengthen security, improve customer experience, and remain competitive in an increasingly digital financial ecosystem.

The future of cooperative banking is not just digital — it is intelligent, secure, and customer-centric. For Urban Co-operative Banks, balancing innovation with trust will be the key to sustainable growth in the years ahead.

Assam Govt partners with BillMart and FynX Capital to launch salary-linked credit for employees

The government of Assam has signed a Memorandum of Understanding (MoU) with BillMart and FynX Capital to introduce Earned Salary Advance (ESA) and Salary-Linked Credit (SLC) facilities for nearly 5 lakh state government employees, marking a significant step toward enhancing financial inclusion and employee welfare.

Launched in Guwahati, the initiative enables government employees to access formal, short-term credit through a secure digital platform, helping them manage immediate financial needs while reducing reliance on informal and high-cost borrowing options.

The agreement aims to deliver these services through a seamless and transparent digital process. The initiative aligns with the vision of Himanta Biswa Sarma, Chief Minister of Assam, to leverage FinTech-driven solutions to improve financial accessibility and employee benefits across the state.

The Chief Minister further stated, "The facility is being delivered through FinAssam, Assam's digital financial platform enabling fast, paperless and transparent credit access for government employees."

The MoU signing was attended by senior government officials, including Chandra Mohan Patowary, Minister for Environment & Forest; Ravi Kota, Chief Secretary; Jayant Narlikar and Virendra Mittal, Commissioners and Secretaries in the Finance Department.

The scheme witnessed strong early traction, with 120 beneficiaries availing the facility within the first 12 hours of launch, facilitating nearly Rs 90 lakh in

credit. The services are being delivered through FinAssam, the state's digital financial platform designed to provide fast, paperless, and transparent credit access.

Under the programme, employees can access a portion of their earned salary before payday through ESA, while also benefiting from salary-linked credit options featuring simplified approval processes and repayment structures integrated with payroll systems.

Sandeep Doshi, Co-founder and COO, BillMart, said the partnership aims to enable responsible, technology-driven financial access for government employees through a secure and user-friendly platform.

Ashok Kumar Mittal, Director, FynX Capital Ltd, highlighted that the focus is on building scalable, technology-driven solutions that don't just provide access, but truly empower the state government employees.

The initiative is being supported by BillMart in collaboration with its financing partner FYNX Capital, ensuring structured and responsible credit delivery.

The launch of ESA and Salary-Linked Credit marks a key milestone in modernising employee financial services in Assam, strengthening access to formal credit, and promoting financial well-being among government employees.

FynX Capital Limited, headquartered in Mumbai, is a technology-driven Non-Banking Financial Company (NBFC) dedicated to democratising credit access for India's Micro, Small, and Medium Enterprises (MSMEs). With more than 1.51 lakh active users, FynX Capital has rapidly emerged as a trusted partner for small businesses and working professionals seeking fast, transparent, and collateral-free financial solutions.

Built on the pillars of adaptability, financial inclusion, fast funding, and fair rates, FynX Capital is committed to bringing underserved borrowers, including small businesses in rural and semi-urban India, into the formal financial ecosystem, while leveraging advanced technology to deliver an accelerated, hassle-free lending experience.

BNG BHARAT™ NETWORK GROUP

Our Publications

The Founder, The Educator and The Banker—three insightful magazines—delivering expert perspectives on business and finance, education, banking and IT, to empower industry leaders and professionals

To Read our Digital Editions,

Log on to: www.bharatnetworkgroup.com

For Print Editions, Contact:

info@thefoundermedia.com

editor@thefoundermedia.com

Announcing

2nd Chapter

CIO HORIZON

Where Vision Becomes Direction

2026

Meet 100+ tech leaders at the industry's most premium summit

3-5 JULY 2026 | RAMADA BY WYNDHAM, HOTEL & CONVENTION CENTER, LUCKNOW

Lucknow

An Initiative of

BNG BHARAT™ NETWORK GROUP

Concept by

Tech Disruptor media.com

For partnership opportunities, please contact

Naman Singhal
naman@thefoundermedia.in
+91 9267933240

Abhinav Chaudhary
abhinav@thefoundermedia.in
+91 8700749849

Engineering the Future of Financial Ecosystem

Where Smart Banking Begins

SIL delivers the complete technology backbone for modern financial institutions. Powering core banking, payments, compliance, lending, and fraud intelligence in one integrated ecosystem.

Our Solutions

Payments
EFT | UPI | POS | ATM
BBPS | AePS

Web-Based Core Banking
Next-Gen mobile banking
Trade Finance |CTS | NEFT, RTGS & IMPS

Digital Lending
LMS | LOS | Collection Engine
BRE | AI-Driven Credit Scoring

Next-Gen Enterprise Solutions
Automated Settlement | Chargeback Settlements | NACH & e-Mandate
Robotic Process | API-Driven CPV & BGV Services

AI Banking
AI/ML Driven Dashboard
360° Reconciliation
AI Based Reports

What Makes SIL Different

Intelligent
AI-powered risk data and decision engines

Interoperable
Seamless APIs across banking ecosystems

Inclusive
Reaching every corner of financial Bharat

Secure
Enterprise-grade protection always on

Our Product Suite

- Web-Based Core Banking
- Payments & Digital Channels
- Cheque Clearing
- Lending & Collections
- Fraud Risk Management
- Enterprise Solutions

sil.co.in