

Banking and Financial Services Rewired

Enabling Trends for India's Intelligent Financial Future

kyndryl

Table of Contents

Future of Banking

- Beyond the “Beep” Your Money is Going Invisible by 2030
- Indian Banking’s Next Frontier: Intelligence at the Core

Regulatory & Compliance

- Regulatory Landscape in India – Current and Emerging
- Embedding Governance in IT Platforms
- Data Privacy and the Impact of the Digital Personal Data Protection (DPDP) Act

Enterprise Architecture

- Enterprise Architecture in BFSI

Security & Resilience

- Embracing Cyber Risk, Regulation, and Resilience: A New Mandate for BFSI Leaders
- From Insight to Impact: How Observability Truly Drives Resilient Banking Experiences
- Securing India’s Digital Payments at Scale: Integrated Fraud Intelligence

Customer Experience

- Designing the Next-Generation Bank Branch: Why Trust, Not Just Technology, Will Define Scale
- From Digital to Contextual: The Next Competitive Frontier for Banks

Sustainable Banking

- AI-Accelerated ESG for India’s Banking and Financial Sector

Kyndryl Agentic AI Framework

- AI-Accelerated ESG for India’s Kyndryl Agentic AI Framework: From Autonomous Agents to Governed Intelligence
  What It Means for India’s BFSI Sector

From Financial Services to the Financial Fabric



Lingraju Sawkar
President, Kyndryl Asia Pacific

In every era, a society is shaped by the systems it trusts enough to stop noticing.

Electricity became transformative only when it turned into a constant-reliable, ubiquitous, and largely invisible. In the decade ahead, finance will follow the same arc. Not because we will "use" banking more, but because it will increasingly behave like a utility of modern life that is embedded in commerce, mobility, and institutions, powering outcomes in the background while citizens and enterprises focus on living and building.

That shift changes the leader mandate. The strategic question is no longer how quickly we can launch the next capability, but what kind of financial fabric we are weaving and whether it can sustain a nation that is scaling in real time.

We are moving toward an economy where value is programmable, decisions are continuous, and risk is instantaneous. In that world, financial institutions become more than providers of products. They become stewards of confidence: confidence that a payment will clear when it matters, that a credit decision will be defensible years later, that a platform will remain dependable under stress, and that innovation will expand opportunity without compromising accountability.

This is where differentiation will be won. Not through louder technology narratives, but through quieter excellence: the ability to design systems that remain trustworthy at speed, absorb shocks without passing it to customers and to ensure that progress remains aligned with societal expectations. The institutions that lead will treat resilience as reputation, responsibility as advantage, and architecture as national-scale enablement.

India has a rare opportunity to set global reference points not only in how fast finance can move, but also in how responsibly it can evolve when the stakes are population-scale. That is the larger context for this compendium. It is an invitation to look beyond near-term playbooks and engage with the deeper questions of the decade: how confidence is engineered, how responsibility is institutionalised, and how financial systems can become a force multiplier for inclusive growth.

Novitas ante portas



Hussain Zaidi,
Kyndryl India

The Banking, Financial Services, and Insurance (BFSI) sector is at a defining inflection point. What was once a steady progression of digitisation has evolved into a fundamental reconfiguration of how financial services are designed, delivered, and governed. Novitas ante portas captures the essence of this moment - innovation is no longer emerging; it is immediate, present, and consequential.

This compendium of perspectives brings together insights from practitioners at the forefront of this transformation. Spanning domains such as artificial intelligence, embedded finance, regulatory evolution, cyber resilience, data governance, enterprise architecture, and customer experience, these contributions collectively reflect the breadth and depth of change underway. More importantly, they articulate a unifying narrative: the future of BFSI will be defined by intelligence, shaped by ecosystems, and sustained by trust.

The boundaries of financial services are rapidly dissolving. Banking is no longer confined to institutions or channels; it is increasingly embedded within the broader fabric of digital interactions - integrated seamlessly into platforms, journeys, and everyday decisions. This shift signals a move from institution-led models to experience-led ecosystems, where value is created contextually and delivered in real time.

At the core of this transformation lies intelligence. The ability to harness data, generate insight, and act with precision at scale is fast becoming the primary determinant of competitiveness. Artificial intelligence is transitioning from isolated use cases to an enterprise-wide capability - reshaping decision-making, strengthening resilience, and enabling a new class of adaptive, anticipatory services.

Yet, as innovation accelerates, the imperative for trust becomes even more pronounced. As financial services become increasingly autonomous and, at times, invisible, governance, transparency, and resilience must scale in parallel. Regulatory compliance, data protection, and cyber risk management are no longer peripheral considerations; they are central to sustaining confidence and enabling long-term growth.

India's BFSI ecosystem offers a uniquely compelling context for this transformation. The convergence of digital public infrastructure, progressive regulatory frameworks, and a rapidly evolving customer base has created conditions for innovation at unprecedented scale. This positions the sector not only to participate in global transformation, but to help define it.

For CxP leaders, the implications are clear. The opportunity extends beyond technology adoption to re-architecting the enterprise - embedding intelligence at the core, strengthening governance by design, and building resilience as a foundational capability. Institutions that succeed will be those that move decisively from digitisation to true transformation - becoming adaptive, predictive, and inherently trusted.

Novitas ante portas is therefore both a reflection and a call to action. Innovation is not approaching - it is here. The imperative now is to engage with it deliberately, strategically, and with clarity of purpose.

This compendium invites you to explore that journey - through perspectives intended to inform decisions, challenge assumptions, and shape the future of financial services.

Future of Banking

Beyond the “Beep” Your Money Is Going Invisible by 2030

Naresh Mehra, Kyndryl India

The Death of the Destination

For the average Indian, the “beep” of a successful UPI transaction is the definitive soundtrack of modern life. In less than a decade, we have transitioned from a cash-dependent society to one where scanning a QR code is a subconscious reflex. Yet, while we celebrate the scan, a more profound “quiet shift” is underway. **We are witnessing the architectural deconstruction of the bank** itself. By 2030, payments will no longer be a destination.

The friction of “going to a bank”-even a digital one-to apply for a loan or insurance will feel like an antiquity. Instead, we are entering the era of invisible finance, where financial services are no longer a separate administrative task but a native, “automatic” layer of our daily existence. Finance is becoming the entry point to everything else, embedded so deeply into our lives that we will stop noticing it entirely.

The “Invisible” Economy: Why You’ll Stop Visiting Banking Apps

The next frontier of India’s economic story is **embedded finance,** a transition from stand-alone banking to services that migrate directly into the platforms where **1 billion Indians** will live, work, and trade. Whether it is an agricultural marketplace or a food delivery app, the bank is receding into the background. This “native” feel is significantly more powerful than traditional banking because platforms already understand user behaviour, risk patterns, and transaction flows better than a bank ever could.

Behind this seamless experience lies a complex technological engine. As highlighted by Magellanic Cloud’s Finoux, the “invisible” gears consist of **cloud-native architectures, AI-driven risk engines, and real-time data pipelines.** These enablers allow credit to appear exactly when a merchant needs working capital or a farmer needs supplies, without a single paper application. As the industry shift suggests: “Making finance work where life already happens.”



The Digital Rupee: It's Not a Bank Account, It's Digital Cash

While digital balances in bank apps are familiar, the RBI's e (Digital Rupee) represents a fundamental shift in the nature of money. The "signal within the noise" here is that the e is a digital bearer instrument-it is a direct liability of the RBI, not a commercial bank deposit.

The RBI Concept Note makes a critical technical distinction: the Token-based logic is preferred for Retail (e-R) because it acts as a bearer instrument (like cash), while the Account-based logic is reserved for Wholesale (e₹-W). This ensures the e retains "cash-like" features:

- **Non-remunerated:** It bears no interest to prevent "disintermediating" the banking system (avoiding a mass migration of funds away from commercial bank deposits).
- **Anonymity:** It offers a degree of privacy for small-value transactions, mirroring physical cash.
- **Settlement Finality:** It eliminates the need for interbank settlement, allowing for instant, risk-free bilateral transfers.

Data as the New Collateral: The Account Aggregator Revolution

The most significant "futurist" signal in India today is the transition from physical assets to Informational Collateral. Through the Account Aggregator (AA) framework, identity and consent-based data sharing are replacing land titles and gold as the foundation of credit. By 2030, India is projected to contribute 47% of the global Open Finance user base, with the domestic user count rising to 479 million. This allows a street vendor with no property to secure a loan based solely on their digital footprint.



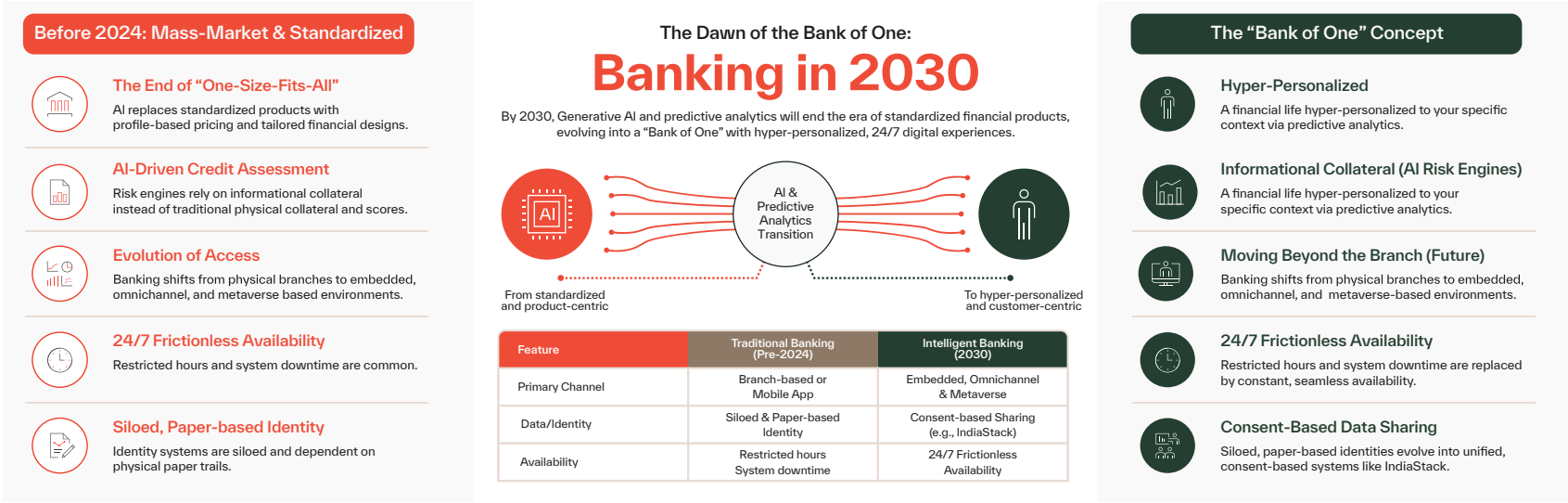
The Rural Frontier: Neobanks are Going to the Farm

The next great fintech frontier isn't the metro; it is the 60 million neobank users expected by 2027 (up from just 6 million in 2021). The bridge to this invisible future is being built by 75 Digital Banking Units (DBUs) across **75 districts,** providing the physical infrastructure for digital-only platforms to thrive in rural India. Neobanks are succeeding where brick-and-mortar failed by designing for the farm, not the boardroom:

Jai Kisan: Its **Bharat Khata app** provides farmers with 10-minute credit approvals in multiple Indian languages.

PayNearby: The **"Digital Naari"** initiative empowers rural women to act as community-driven inclusion hubs, bringing banking to the doorstep.
These models prove that when you remove the branch and replace it with a tailored app, you don't just provide an account; you provide a livelihood.

Hyper-Personalization: The AI-Driven "Bank of One"



In this future, freelancers will access "gig economy loans" that flex with their monthly income, and homebuyers might navigate "metaverse mortgages" for virtual and physical properties alike.

The Road to $7 Trillion

These shifts are the primary engines driving India toward its **$7 trillion GDP** aspiration by 2030. It is a staggering trajectory: while India targets a $ 7 trillion economy, embedded finance alone is projected to hit **$7 trillion in transaction value globally by the end of the decade.**

As finance becomes invisible-embedded in every scan, harvest, and digital interaction-our relationship with "the bank" changes. The bank is no longer a place we go; it is a trusted system that is everywhere and nowhere at once.

However, as the system becomes invisible, accountability must become visible. With the **Digital Personal Data Protection (DPDP)** Act providing the guardrails, the next decade will be defined not by who builds the most apps, but by who designs the most trusted systems. As we move toward 2030, the question for the consumer is no longer "Where is my bank?" but "How well does my money understand my life?

Future of Banking

Indian Banking's Next Frontier: Intelligence at the Core

Hussain Zaidi, Kyndryl India

Artificial Intelligence (AI) is fast evolving to be the defining force that determines how financial institutions compete, scale, and stay relevant. As customer expectations evolve in real time and digital ecosystems grow more complex, an AI-focused digital strategy is becoming a foundational need for modern banking.

India's digital financial infrastructure has created the conditions for this shift. Platforms such as UPI, Aadhaar, and consent-based data sharing frameworks generate unprecedented volumes of real-time, high-quality data. AI transforms this data into insight, enabling banks to understand customer intent, anticipate needs, and act with speed and precision.

India's banking customers are taking a digital-first approach and they need their services to be intuitive, responsive, and secure by default. Interactions are expected to be seamless and personalised, whether it be instant payments, contextual credit offers, or real-time fraud prevention.

It is no longer possible to enable this at scale through rule-based systems or legacy operating models alone. Without artificial intelligence embedded at the core, digital infrastructure alone cannot deliver differentiated experiences.

A New Definition of Banking Experiences

Banking transformation over the years has focused on efficiency and channel expansion, the next phase of which will be intelligence-driven experiences where banks move from responding to customer actions to predicting them. AI enables this transition by continuously learning from behaviour, context, and risk signals across touchpoints.

This shift is already visible across the sector. The 2025 Kyndryl Readiness Report highlights that a large majority of banking leaders expect AI to significantly reshape roles, operations, and decision-making in the near term signalling a clear industry consensus that intelligence will be central to future competitiveness.

The payments segment is a great example of what began as a transactional ecosystem rapidly evolving into an intelligent one, where nudges, safeguards, and value-added services are informed by real-time analysis. Similar transitions are underway in lending, wealth management, and customer service, as banks explore AI-powered credit assessment, advisory tools, and automated decision-making.





Intelligence Thrives on Interoperability

Many banks still continue to operate in hybrid environments, combining modern platforms with legacy core systems. AI solutions can address these complexities by unifying data across environments, improving system observability, and supporting large-scale modernisation without disrupting critical operations.

AI delivers its full value when banking systems are connected, interoperable, and resilient. India's digital public infrastructure provides a unique advantage by enabling banks, fintechs, and regulators to operate on shared rails. Identity, payments, and data exchange frameworks create an environment where intelligent systems can function at national scale.

Responsibility is Now Part of Innovation

As AI becomes embedded in core banking processes, trust and governance must scale alongside innovation. Intelligent systems influence credit decisions, detect fraud, and shape customer engagement making transparency, fairness, and resilience essential.

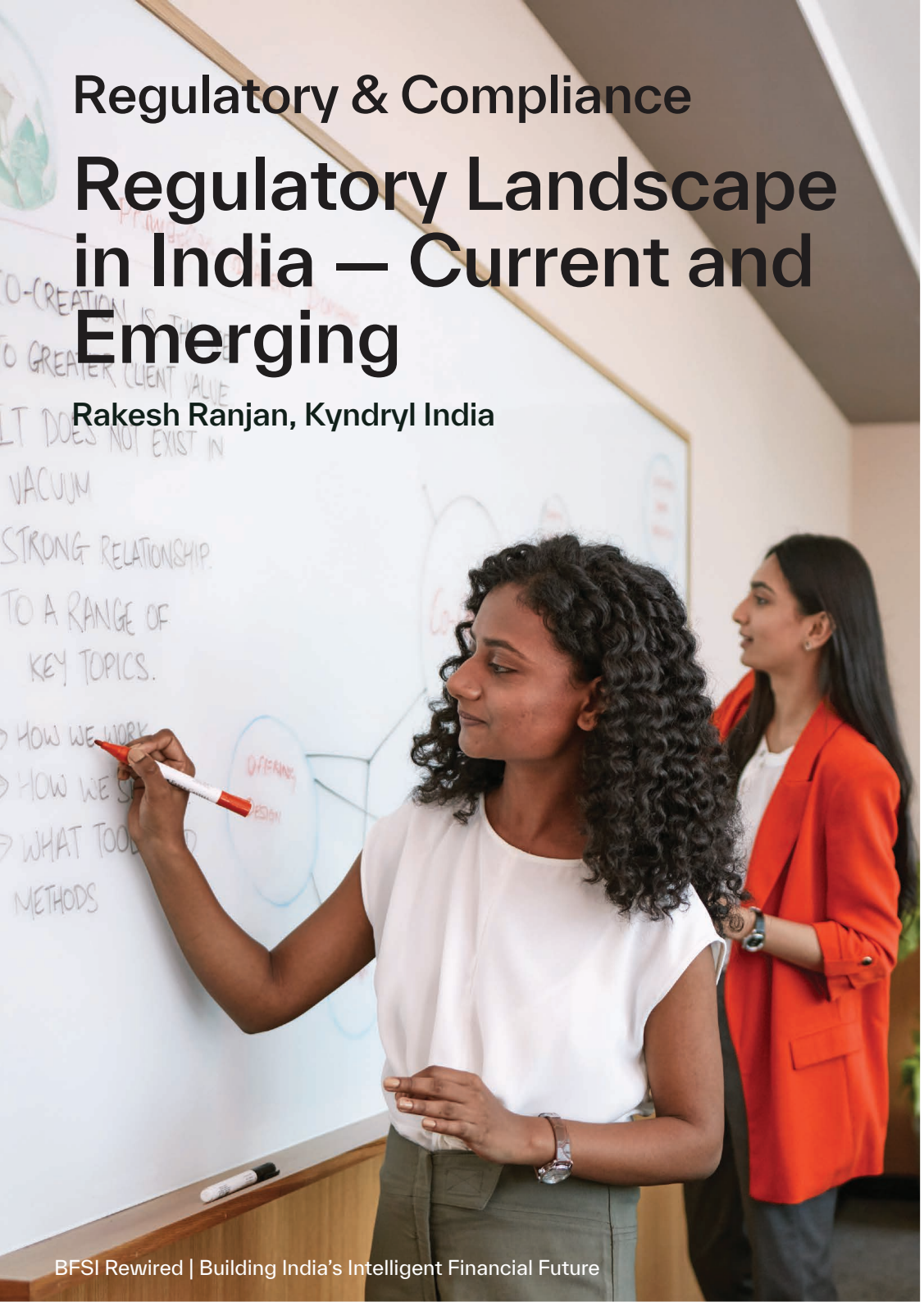
Banks must therefore strengthen AI governance frameworks, ensure explainability in decision-making, and design architectures that remain robust amid cyber threats and operational disruptions. In this environment, responsible AI is not a regulatory checkbox but a prerequisite for sustainable growth.

The Way Forward: Intelligence at the Core

The future of Indian banking will not be defined by who launches the next digital feature first. It will be shaped by those that embed intelligence deeply across their operations using AI to improve decision-making, strengthen resilience, and anticipate customer needs with accuracy.

Banks that succeed will move beyond digitisation to become truly intelligent enterprises. India has the ecosystem, talent, and policy momentum to lead this shift globally.

The question is no longer whether AI will reshape banking. It is whether banks are ready to place intelligence at the core of everything they do.



Regulatory & Compliance

Regulatory Landscape in India — Current and Emerging

Rakesh Ranjan, Kyndryl India

India's financial sector is at the crossroads of rapid technological advancements, changing consumer habits, and an increasingly interconnected global economy. Over the last decade, these forces have sped up the transformation of the country's banking and financial services landscape. As digital payment systems, fintech innovations, and new business models emerge, the regulatory framework supporting this sector has adapted.

At the heart of these changes is the Reserve Bank of India (RBI), whose actions and reforms have shaped not only the rules for financial institutions but also the sector's growth and resilience. This document explores the evolving financial regulatory environment in India, focusing on the RBI's regulation strategies, recent reforms, digital transformation, risk management, financial inclusion, and the perspectives of major market players. The analysis aims to provide finance professionals, policymakers, and researchers with a thorough understanding of India's current regulatory landscape.

The Reserve Bank of India's Evolving Regulatory Approach

As India's central bank and principal regulator of the banking sector, the RBI has long been tasked with maintaining monetary stability, supervising financial institutions, and protecting consumer interests. However, the past decade has brought new challenges, including the rise of digital financial services, cross-border capital flows, and systemic risks posed by non-traditional players. In response, the **RBI has transitioned from a reactive regulatory stance to a more proactive, anticipatory approach.** This shift is evident in its deployment of forward-looking frameworks, data-driven supervision, technology-driven platforms, and ongoing stakeholder engagement.

Recent years have witnessed the RBI introducing a suite of regulatory reforms aimed at strengthening the financial system's resilience while fostering innovation through the Reserve Bank Innovation Hub (RBIH). These measures have spanned the introduction of differentiated banking licenses, enhanced prudential norms for various financial entities, and a reimagined approach to fintech regulation through appointing FACE (Fintech Association for Consumer Empowerment) as an SRO (Self-Regulatory Organization). The RBI's willingness to adapt its oversight, consult industry participants, and pilot regulatory sandboxes exemplifies its commitment to balancing stability with growth.

Regulation of Digital Payments and Fintech

The proliferation of digital payments in India has been one of the defining trends of the last decade. Catalyzed by government initiatives such as demonetization and the Digital India program, the volume and value of electronic transactions have surged. The Unified Payments Interface (UPI), launched under the aegis of the National Payments Corporation of India (NPCI) with the RBI's support, has revolutionized peer-to-peer and merchant payments, making India a global leader in real-time payment systems.

Recognizing the opportunities and risks inherent in this digital revolution, the RBI has taken decisive steps to regulate the digital payments ecosystem. Its guidelines mandate strong customer authentication, promote interoperability among wallets and banks, protect customers' digital personal data, and establish frameworks for grievance redressal. To address cybersecurity concerns, the RBI has issued detailed directives on data localization, fraud monitoring, and incident reporting, compelling payment service providers to invest in robust security infrastructure.

Additionally, the RBI has encouraged responsible innovation by establishing clear licensing regimes for payment aggregators and payment gateways. The Payment and Settlement Systems Act 2007, along with periodic circulars, sets out the operational and prudential standards for both bank-led and non-bank payment entities. The regulator's consultative approach, involving public feedback and industry dialogue, has helped create an environment that supports competition, performance, and consumer protection.

The fintech sector, encompassing lending platforms, robo-advisors (Wealth Tech, Reg Tech, Personal Finance Management, etc.), wallets, and neobanks, has also attracted regulatory attention. The RBI has clarified its stance on digital lending, issuing guidelines to curb predatory practices (e.g. FLDG), ensure transparency in loan terms, and enforce fair collection methods. Regulatory sandboxes, launched in 2019, allow fintech firms to test new products in a controlled environment, facilitating innovation while managing systemic risks. These initiatives underscore the RBI's role as an enabler of digital transformation, rather than merely a gatekeeper.

Oversight of Non-Banking Financial Companies (NBFCs)

Non-banking financial companies (NBFCs) play a crucial role in India's credit system by serving segments often ignored by banks. Recent liquidity stresses exposed weaknesses in governance, asset quality, and risk management. The RBI has responded by tightening regulations, aligning NBFC standards with those of banks while recognizing their unique models. Reforms include higher capital requirements, stricter asset classification, and quick corrective actions for struggling NBFCs. The RBI also mandated independent directors, enhanced disclosures, and improved risk management policies to increase transparency, encourage responsible lending, and safeguard depositors.

To prevent regulatory gaps, the RBI has harmonized norms like liquidity and large exposure limits. It closely monitors systemically important NBFCs, conducting stress tests and inspections to ensure they support financial inclusion without risking systemic stability.

Financial Inclusion and Consumer Protection

Achieving inclusive growth remains a cornerstone of India's financial sector strategy. The RBI has played a pivotal role in extending formal financial services to unbanked and underbanked populations, especially in rural and semi-urban areas. The introduction of differentiated banking models, such as payments banks and small finance banks, has expanded access to savings, payments, and credit products for millions of new customers. One of the most significant recent initiatives is the Account Aggregator framework, which empowers individuals to securely share their financial data across institutions with their consent. By facilitating data-driven credit assessment, the framework enables lenders to better serve thin-file customers, thereby reducing information asymmetry and broadening credit access.

The RBI has also championed regulatory sandboxes to foster experimentation with new financial products and services in a controlled environment. These sandboxes allow fintechs, banks, and NBFCs to test innovations-such as alternative credit scoring, digital KYC solutions, and blockchain applications-under regulatory supervision. The lessons learned inform future policy development and risk mitigation.

Consumer protection is embedded in the RBI's regulatory philosophy. The regulator has mandated fair disclosure of product terms, established ombudsman schemes for grievance redressal, and introduced guidelines to curb mis-selling and predatory lending. Financial literacy initiatives, often conducted in partnership with industry bodies and civil society, complement these efforts by empowering consumers to make informed financial decisions.



Perspectives from Financial Institutions

Financial institutions operating in India-spanning public and private sector banks (all types of differentiated banks), NBFCs, cooperative banks, and fintech startups-have had to recalibrate their strategies in response to the evolving regulatory environment. The increasing complexity of compliance requirements, coupled with the pace of regulatory change, has prompted significant investment in technology, talent, and risk management systems.

Banks and NBFCs are leveraging regulatory technology (RegTech) solutions to automate compliance monitoring, reporting, and fraud detection. By integrating artificial intelligence and machine learning into their workflows, these institutions can identify emerging risks, ensure timely regulatory filings, and enhance audit readiness. Fintech companies, meanwhile, are engaging proactively with regulators through industry associations and public consultations, seeking clarity on evolving guidelines and contributing to policy development.

The collaborative dynamic between regulators and market participants is evident in joint projects and pilot initiatives. For example, several banks, fintechs, and academia have participated in the RBI's regulatory sandbox cohorts, testing innovations in cross-border payments, identity verification, and micro-lending. These engagements have fostered a culture of shared responsibility for risk management and consumer protection.

However, the evolving regulatory landscape is not without challenges. Institutions must balance the imperative to innovate with the need to adhere to stringent compliance standards. Smaller NBFCs and startups may face resource constraints in implementing advanced risk management frameworks. Nonetheless, many view the regulatory environment as an opportunity to differentiate themselves through transparency, governance, and customer-centricity.

Opportunities and Challenges

The RBI's regulatory reforms have created fertile ground for innovation in areas such as digital lending, open banking, and embedded finance. The push for interoperability and data portability-exemplified by the UPI and Account Aggregator frameworks-enables new business models that leverage ecosystem partnerships and network effects.

Digital lending, for instance, has expanded rapidly, with fintechs and banks collaborating to offer instant, tailored credit products to individuals and small businesses. The RBI's guidelines on digital lending, covering issues such as loan sourcing, data privacy, and disclosure, aim to promote responsible growth and mitigate risks related to over-leverage and data misuse. Open banking initiatives, backed by API standardization and data-sharing protocols, are fostering greater competition and financial inclusion. Institutions can offer customers a unified view of their financial relationships, facilitate seamless switching of service providers, and deliver personalized financial advice. The RBI's consultative approach to open banking regulation reflects a recognition of its transformative potential, as well as the need for robust data protection mechanisms.

Despite these opportunities, several challenges persist. Cybersecurity threats, privacy risks for personal data, operational risks, and digital fraud require ongoing vigilance and coordination between regulators and market participants. The rapid pace of technological change can outstrip regulatory capacity, necessitating continuous upskilling of supervisory staff and agility in rulemaking. Furthermore, the uneven adoption of digital solutions across regions and demographic groups raises concerns about digital exclusion and the need for targeted financial literacy programs.

Cross-border regulatory issues, such as data localization requirements and anti-money laundering compliance, add another layer of complexity for multinational banks and fintechs operating in India. The RBI's engagement with international standard-setting bodies and adoption of global best practices are critical to ensuring that India's regulatory framework remains fit for purpose in a globalized financial system.

Key Trends and Outlook



Focus on Digital Transformation

The regulatory agenda has accelerated the adoption of digital payments, e-KYC, and online lending, positioning India as a leader in digital financial services. The integration of technologies such as artificial intelligence, blockchain, and biometrics is expected to further enhance operational efficiency and customer experience.



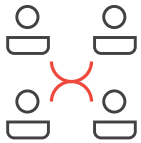
Strengthening Risk and Compliance

Enhanced scrutiny of asset quality, liquidity, and governance is prompting institutions to upgrade their risk management frameworks. The RBI's emphasis on stress testing, scenario analysis, and early warning systems aims to preempt systemic shocks and promote resilience.



Emphasis on Financial Inclusion

Regulatory initiatives such as differentiated banks, microfinance reforms, and the Account Aggregator framework are expanding access to financial services for underserved populations. The use of digital channels and agent networks is bridging geographic and socio-economic divides.



Collaborative Policy Development

The RBI's consultative approach, involving dialogue with industry associations, consumer groups, and technology experts, fosters a more adaptive and responsive regulatory environment. Policy experimentation through regulatory sandboxes and pilot projects supports evidence-based rulemaking.



Sustainable Finance and ESG Integration

Emerging trends include integrating environmental, social, and governance (ESG) considerations into lending and investment decisions. The RBI has signaled its intent to develop frameworks for green finance and climate risk management, aligning Indian regulations with global sustainability goals.



Cross-Border and Global Alignment

As Indian financial institutions expand overseas, and global entities enter the domestic market, the RBI is increasingly harmonizing its regulations with international standards. This includes participation in forums such as the Basel Committee on Banking Supervision and Financial Stability Board.

The Way Forward

In summary, the evolving regulatory landscape in India's financial sector reflects a delicate balance between fostering innovation and ensuring systemic stability. The Reserve Bank of India's proactive agenda has catalyzed digital transformation, strengthened risk controls, and promoted financial inclusion, placing the country at the forefront of digital finance globally. However, this rapid evolution brings with it significant challenges, such as cybersecurity threats, operational risks, and the complexities of cross-border compliance, all of which demand continuous adaptation by both regulators and market participants.

The RBI's collaborative and consultative approach-drawing on industry expertise, international standards, and policy experimentation-has proven essential in navigating these complexities and maintaining market confidence. As sustainability and ESG considerations become increasingly central, India's integration of green finance and climate risk management frameworks will further align its financial system with global priorities.

Ultimately, sustained investment in regulatory capacity, technology infrastructure, and financial literacy will be crucial to ensuring that the gains from innovation are shared broadly, risks are mitigated, and the financial sector remains resilient and inclusive in the face of ongoing change. This holistic approach positions India well to address future challenges and seize new opportunities in the dynamic world of finance.

> "AI is here to stay, but banks should resist the pressure to implement it simply because everyone else is doing it. The real priority is consolidating and standardizing data, strengthening DPDP and automation foundations, and becoming AI-ready before pursuing large-scale AI deployments."



Vikas Deshmukh
CTO, Suryoday Bank



Regulatory & Compliance

Embedding Governance in IT Platforms

Rakesh Ranjan, Kyndryl India

Why governance is now as important as scale in the digital platform era.

Large IT platforms now sit at the center of modern life. They power commerce, communication, public services, payments, cloud operations, and vast parts of the digital economy. They do more than support transactions. They shape how information moves, how people interact, how businesses compete, and how institutions deliver services. As these platforms grow in scale and influence, one reality becomes impossible to ignore: technology alone cannot sustain trust. Governance has to do that.

That is why governance in large IT platforms has become a strategic issue rather than a procedural one. The question is no longer simply whether a platform works. It is whether it operates transparently, responsibly, securely, and in a way that balances innovation with accountability. In complex digital ecosystems, governance is what turns scale into something durable. Without it, scale can just as easily become a source of risk, opacity, and institutional fragility.

At its core, governance is about how platforms are guided, controlled, and evolved. It includes the policies, decision rights, structures, controls, and oversight mechanisms that shape how a platform functions and how it responds to stakeholders, regulators, and society at large. Unlike traditional organizational governance, platform governance operates in a far more demanding environment. It must account for multiple stakeholders, rapid technological change, global operations, constant data flows, and the challenge of managing both economic and social consequences at once.

Certain principles sit at the heart of this. Transparency matters because users and stakeholders increasingly expect to understand the rules that shape their digital experience. Accountability matters because platforms cannot operate at scale without mechanisms for grievance handling, oversight, and consequence management. Inclusivity matters because these ecosystems affect far more people than the organizations that own them. Adaptability matters because risks evolve faster than static controls can keep up. And ethical stewardship matters because platforms now influence privacy, safety, competition, and digital well-being in ways that have real societal consequences.

One of the most useful distinctions in this conversation is the difference between platform governance and process governance. The two are related, but they are not the same.

Platform governance is concerned with the ecosystem itself. It defines how the platform operates, how participants interact with it, what kinds of behavior are allowed, how data is managed, how fairness is preserved, and how regulatory obligations are met. It is strategic and outward-facing. It shapes the architecture of trust across the platform's entire environment. Process governance, by contrast, focuses on the discipline of internal execution. It deals with workflows, standard operating procedures, performance measurement, operational risk, and continuous improvement. One governs the platform as a living ecosystem. The other governs the machinery that keeps it running well. Both matter. Confusing them weakens both.

For governance to be effective at platform scale, several elements need to be in place. There must be a formal governance framework with defined roles, responsibilities, and decision-making authority. Policies for participation, moderation, privacy, and security need to be clear, accessible, and regularly updated. Enforcement mechanisms must exist to monitor compliance, investigate violations, and act when rules are broken. Transparency cannot be performative; it must be backed by reporting, disclosure, and auditability. And stakeholder engagement has to be real, because legitimacy is far stronger when governance is shaped with, not merely imposed on, the communities a platform serves.

Technology can support these goals, but it cannot substitute for them. Automation, AI, and machine learning can help identify anomalies, flag harmful content, improve monitoring, and streamline compliance activity. Yet those tools themselves must be governed. A platform cannot claim strong governance while operating opaque automated systems that affect rights, access, or outcomes without clear standards or recourse. The governance challenge does not disappear when machines are introduced. It often becomes more important.

The difficulty, of course, lies in the nature of the platforms themselves. Their global reach means they often operate across conflicting regulatory environments. Their pace of innovation means governance frameworks are frequently catching up rather than leading. Their dependence on data creates constant privacy and security pressures. Content moderation remains one of the most difficult balancing acts in digital governance, sitting between safety, legality, and freedom of expression. And as platforms become larger, questions of market power, concentration, and fairness become impossible to separate from governance itself.



This is especially important in the context of Digital Public Infrastructure. DPI systems such as digital identity, payment rails, and public data platforms are not just commercial systems. They underpin public trust, citizen access, and economic participation. Governance in these environments has to meet an even higher bar because failures do not stay contained within a user base or a market segment. They affect citizens, inclusion, state credibility, and the functioning of essential services. Inadequate governance in DPI can lead to privacy harm, exclusion, misuse, and erosion of trust in institutions themselves. That makes governance not a technical afterthought, but a foundational requirement for inclusive digital transformation.

The best approaches emerging today tend to share a few characteristics. They bring multiple stakeholders into the governance process rather than concentrating authority too narrowly. They place user rights, safety, and privacy at the center of design. They make decisions and enforcement actions more visible rather than hiding them behind platform opacity. They support interoperability and open standards where possible, reducing lock-in and strengthening resilience. And they stay adaptive, because fixed governance models struggle in environments shaped by constant technological and social change.

> “As India’s BFSI sector accelerates toward a digital-first future, the next phase of transformation will be defined not just by innovation, but by resilience, trust, and adaptability.
>
> The winners will be those who can balance speed with stability while continuously evolving with regulatory and customer expectations.”



Abdul Hameed
Deputy Chief Technology Officer,
Ujjivan Small Finance Bank

The future will make this even more urgent. Artificial intelligence, the Internet of Things, decentralized systems, and growing demands for algorithmic accountability will only expand the governance burden on large platforms. Governments will increase scrutiny. Users will expect more transparency. Civil society will demand more ethical responsibility. Platforms will need to become more participatory in how they are governed, even as they remain agile enough to innovate.

In the end, governance is what determines whether a platform can remain trusted as it grows more powerful. It is the discipline that keeps scale aligned with societal value. It is the mechanism through which innovation earns legitimacy. And in a world increasingly shaped by large digital systems, it may be the single most important difference between platforms that merely expand and platforms that endure.

Data Privacy and the Impact of the Digital Personal Data Protection (DPDP) Act

Rakesh Ranjan, Kyndryl India

Overview of the Digital Personal Data Protection Act, 2023

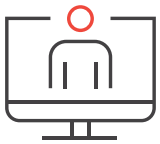
Data privacy is crucial for trust and security as technology changes how personal information is handled. The increase in digital transactions, cloud services, and data exchanges raises the risks of breaches and misuse. The Government of India introduced the Digital Personal Data Protection Act (DPDPA) in 2023 to establish a framework for personal data protection, address compliance issues, and enhance regulation. This report examines the DPDPA, India's data privacy landscape, gaps in compliance and enforcement, and the actions needed from the industry and regulators to ensure effective data protection.

The Digital Personal Data Protection Act represents a pivotal piece of legislation in India's data governance ecosystem. Its primary objective is to provide individuals with greater control over their personal data while ensuring that organizations that process it adhere to rigorous standards of transparency, accountability, and security. The Act applies to both government and private entities that process digital personal data within India, as well as to entities outside India that process data in connection with activities related to offering goods or services to individuals



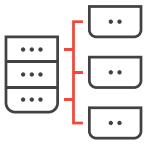
Key Provisions and Objectives

Through these provisions, the DPDPA seeks to balance individual privacy rights with the legitimate interests of businesses, fostering a culture of responsible data stewardship and enhancing India's global standing in data protection.



Consent-Based Data Processing

The Act mandates that personal data should only be processed with the explicit consent of the customer, except in specific circumstances defined by law, for e.g., national security, legal obligations.



Data Principal Rights

Individuals (customers) are empowered with rights to access, correct, erase, and port their personal data, and to withdraw consent at any time.



Obligations of Data Fiduciaries

Organizations processing personal data (referred to as data fiduciaries) must implement technical and organizational measures to ensure data security, maintain data accuracy, and prevent unauthorized processing.



Data Protection Board

The Act establishes an independent Data Protection Board tasked with over-seeing compliance, investigating breaches, and imposing penalties for violations.



Cross-Border Data Transfers

The Act regulates the transfer of personal data outside India, subjecting it to conditions prescribed by the government to ensure adequate protection standards.



Penalties and Remedies

Stringent penalties are prescribed for non-compliance, including substantial fines for data breaches, failure to comply with data principal rights, and other contraventions.

Current Data Privacy Landscape in India

Prior to the enactment of the DPDPA, India's data privacy regime was governed by a patchwork of sectoral regulations and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, under the Information Technology Act, 2000. While these frameworks provided a foundational level of data protection, they lacked the comprehensiveness and enforceability necessary to address the complexities of modern digital ecosystems.

Financial institutions, telecom operators, healthcare providers, and other critical sectors were subject to additional data protection mandates issued by their respective regulators. However, the absence of a unified, overarching data protection law led to inconsistencies in compliance standards, enforcement, and redressal mechanisms. Additionally, the rapid adoption of digital technologies outpaced the evolution of regulatory frameworks, resulting in significant vulnerabilities and challenges in safeguarding personal data.

Existing Frameworks and Challenges

Fragmented Regulatory Approach

Multiple sector-specific guidelines created confusion and compliance burdens for organizations operating across industries.

Limited Enforcement Capacity

Regulatory authorities often faced resource constraints and lacked the technical expertise to effectively monitor and penalize non-compliance.

Inadequate Consumer Awareness

Many individuals remained unaware of their data privacy rights and the risks associated with digital transactions.

Technological Evolution

The rise of artificial intelligence, big data analytics, and cloud computing introduced new complexities in data management and security.

Through these provisions, the DPDPA seeks to balance individual privacy rights with the legitimate interests of businesses, fostering a culture of responsible data stewardship and enhancing India's global standing in data protection.



Gaps in Data Privacy

Despite the progress made with the introduction of the DPDPA, several gaps persist in India's data privacy landscape. Addressing these gaps is critical to realizing the full potential of the Act and ensuring the protection of personal data in an increasingly digital society.

Compliance Issues

- **Inconsistent Implementation:** Organizations vary in their maturity and resources to implement comprehensive data privacy programs, leading to uneven compliance across sectors.
- **Legacy Systems:** Many organizations continue to rely on outdated IT infrastructure that lacks modern security features, making compliance with new standards challenging.
- **Third-Party Risk:** The increasing reliance on third-party vendors and service providers introduces additional risks, as organizations may have limited visibility or control over how data is handled outside their direct environment.

Enforcement Challenges

- **Resource Constraints:** Regulatory bodies, including the Data Protection Board and sectoral regulators, require significant investments in capacity building, technology, and personnel to enforce the DPDPA effectively.
- **Jurisdictional Overlaps:** Overlapping mandates between central and state authorities, as well as sectoral regulators, may lead to conflicts and delays in enforcement actions.
- **Redressal Mechanisms:** The establishment of accessible and efficient mechanisms for individuals to report violations and seek remedies remains a work in progress.

Technological Limitations

- **Rapid Innovation:** The pace of innovation in data-driven technologies often outstrips the ability of regulatory frameworks to keep up, resulting in regulatory lag.
- **Data Localization vs. Global Operations :** Requirements for data localization may conflict with the operational realities of multinational organizations, leading to compliance complexities and increased costs.
- **Security Skills Gap:** There is a shortage of skilled professionals in data security and privacy, limiting the ability of organizations to implement advanced protection measures.

These gaps highlight the need for a coordinated, forward-looking approach by both the industry and regulators to ensure sustained compliance and effective protection of personal data.

Necessary Industry Actions

The successful implementation of the DPDPA hinges on the proactive engagement of industry stakeholders. Organizations must go beyond mere compliance to foster a culture of data privacy and security that permeates every aspect of their operations.

Compliance Strategies

- **Comprehensive Data Mapping:** Organizations should conduct thorough data mapping exercises to identify the types, sources, and flows of personal data within their systems, including data shared with third parties.
- **Privacy Impact Assessments:** Regular assessments should be conducted to evaluate the privacy risks associated with data processing activities and to implement mitigation measures.
- **Policy Development:** Clear and transparent privacy policies, aligned with the DPDPA's requirements, must be communicated to customers, employees, and other stakeholders.
- **Record Keeping:** Meticulous documentation of consent, data processing activities, and data subject requests is essential for demonstrating compliance during audits and investigations.

Data Governance

- **Establishing Data Governance Frameworks:** Organizations should implement governance structures that define roles, responsibilities, and accountability for data privacy across functions.
- **Appointment of Data Protection Officers:** Designating qualified officers to oversee data protection initiatives and ensure ongoing compliance is recommended, especially for organizations handling large volumes of sensitive data.
- **Internal Audits:** Periodic audits of data processing activities should be conducted to identify gaps, monitor compliance, and drive continuous improvement. report violations and seek remedies remains a work in progress.

Employee Training

- **Awareness Programs:** Regular training sessions should be organized to educate employees about their obligations under the DPDPA and best practices for handling personal data.
- **Incident Response Training:** Employees must be trained to recognize and respond effectively to data breaches, ensuring that incidents are reported promptly and managed appropriately.
- **Role-Based Training:** Tailored training should be provided to employees based on their roles and access to sensitive data, with a focus on high-risk functions such as IT and customer service.

Technology Adoption

- **Data Security Technologies:** Implementation of encryption, access controls, intrusion detection systems, and secure authentication mechanisms is vital to safeguard personal data.
- **Automation Tools:** Automation can streamline compliance processes, such as consent management and data subject request handling, thereby reducing the risk of human error.
- **Continuous Monitoring:** Real-time monitoring of data flows and security events enables organizations to detect and respond to threats proactively.

By embedding these actions into their operational fabric, industry players can not only comply with regulatory requirements but also build customer trust and competitive advantage.

Role of the Regulators

The regulators across various domains play a pivotal role in shaping data privacy standards and ensuring the secure handling of personal data by financial institutions. Regulators' responsibilities are multifaceted, encompassing regulatory, supervisory, and advisory functions.

Regulatory Expectations

- **Issuing Guidelines:** Regulators are expected to issue detailed guidelines to regulated institutions, outlining the specific obligations and compliance measures required under the DPDPA.
- **Sector-Specific Standards:** Tailoring data privacy standards to address the unique risks and operational realities of the banking and financial sector is essential.
- **Promoting Best Practices:** The regulators should advocate for the adoption of global best practices in data privacy and security, fostering a culture of continuous improvement.

Supervisory Actions

- **Monitoring Compliance:** The regulators must establish robust supervisory mechanisms to monitor compliance with data privacy regulations, including periodic audits and inspections.
- **Enforcement and Penalties:** Clear enforcement protocols and penalties for non-compliance should be articulated to ensure accountability across the sector.
- **Incident Reporting:** Regulated institutions should be required to report data breaches and privacy incidents to the respective in a timely manner, enabling coordinated responses and sector-wide learning.

Guidance for Regulated Institutions

- **Capacity Building:** The regulators should support institutions in building internal capacity for data privacy compliance, including training, resource allocation, and technology adoption.
- **Facilitating Collaboration:** Encouraging collaboration between banks, fintech companies, and other stakeholders can drive innovation while ensuring compliance with privacy standards.
- **Engagement with Stakeholders:** Ongoing engagement with industry associations, consumer groups, and technology providers is vital for identifying emerging risks and refining regulatory approaches.

Through these actions, regulators can reinforce their leadership in safeguarding the integrity and security of the financial ecosystem while aligning with the broader objectives of the DPDPA.

Recommendations: Bridging Gaps and Advancing Data Privacy

To realize the vision of robust data privacy protection, both the industry and the regulators must undertake coordinated, strategic actions. The following recommendations are designed to bridge existing gaps and foster a resilient data privacy environment in India.

For Industry

- **Invest in Technology:** Allocate resources to advanced data security technologies to futureproof, including encryption, threat intelligence, and automation tools.
- **Strengthen Vendor Management:** Establish stringent due diligence and monitoring processes for third-party vendors to ensure compliance throughout the data lifecycle.
- **Enhance Transparency:** Clearly communicate privacy practices to customers and internal staff to foster informed consent and build trust.
- **Foster a Privacy Culture:** Integrate data privacy considerations into all aspects of business operations, from product design to customer support.
- **Engage in Continuous Improvement:** Regularly review and update privacy policies, procedures, and technologies to keep pace with evolving threats and regulatory requirements.

For the Regulator

- **Develop Comprehensive Guidance:** Issue sector-specific guidance documents and FAQs to clarify DPDPA compliance requirements for financial institutions.
- **Leverage Technology in Supervision:** Invest in supervisory technology (SupTech) to enhance monitoring and proactively detect non-compliance.
- **Facilitate Industry Collaboration:** Organize forums, workshops, and knowledge-sharing platforms to promote best practices and collective problem-solving.
- **Support Research and Innovation:** Encourage the development of privacy-enhancing technologies and support pilot projects that demonstrate innovative approaches to data protection.
- **Monitor Global Trends:** Stay abreast of international developments in data privacy and adapt regulatory approaches to align with global standards.

> “The BFSI sector is entering a defining phase of structural transformation. AI, intelligent automation, and rising customer expectations are rewriting operating models, from credit decisioning and risk management to omnichannel journeys and hyper-personalisation.”



George John
Executive Director, ESAF Small Finance Bank

Best Practices

- Adopt a risk-based approach to data privacy management, prioritizing resources based on the sensitivity and criticality of data assets.
- Implement data minimization principles, collecting and retaining only the data necessary for legitimate business purposes.
- Regularly test and update incident response plans to ensure swift and effective management of data breaches.
- Engage with external experts and auditors to validate privacy and security controls.
- Promote consumer awareness through targeted outreach and education initiatives.

The Way Forward

The enactment of the Digital Personal Data Protection Act marks a transformative moment in India's journey toward a secure and privacy-centric digital economy. While the act lays a strong foundation, its success depends on the collective efforts of industry players, regulators, and policymakers to bridge existing gaps, embrace technological innovation, and foster a culture of accountability and transparency.

The industry must take concrete steps to operationalize privacy principles, while regulators must provide clear guidance, robust supervision, and strategic leadership. By working together, stakeholders can ensure that data privacy is not just a regulatory obligation but a fundamental value that underpins trust, innovation, and sustainable growth in the digital age.



Enterprise Architecture in BFSI

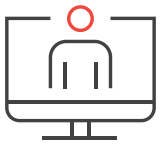
Tejas Desai, Kyndryl India

In Banking, Financial Services, and Insurance (BFSI), Enterprise Architecture (EA) is the discipline that structures and governs how business capabilities, regulatory obligations, and technology platforms work together at scale, while ensuring security, resilience, and compliance.



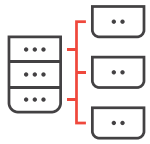
Enterprise Architecture in BFSI

In summary, in BFSI, Enterprise Architecture is the structured practice of aligning banking and insurance business capabilities with secure, compliant, and resilient technology platforms, enabling institutions to innovate, scale, and meet regulatory obligations without increasing risks.



Business-IT Alignment under Regulation

EA ensures business goals are translated into secure, compliant IT systems that meet regulatory and risk requirements.



Core System-Centric Design

EA is built around core banking/insurance systems and integrates channels, payments, CRM, and data platforms.



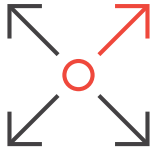
Security and Compliance by Design

Security, risk, AML, and regulatory controls are embedded into the architecture from the start.



High Availability and Resilience

EA ensures continuous operations through disaster recovery, redundancy, and scalable infrastructure.



Safe Digital Transformation

EA enables cloud, APIs, AI, and digital channels while protecting legacy systems.

Architectural Framework

The Architectural Framework establishes Enterprise Architecture (EA) as the central governance and decision making function that ensures technology solutions consistently align with business strategy, regulatory requirements, and enterprise standards.

At the core of the framework, Enterprise Architecture provides a single architectural lens through which business needs, technology choices, and risk considerations are assessed and governed.



Requirements and Reviews

This stage captures and continuously manages functional and non functional requirements, including performance, security, scalability, availability, and compliance.

Architecture reviews ensure that evolving requirements remain aligned with enterprise standards and regulatory expectations.

Overview and Design

The framework defines a structured approach to system context definition, architectural overview, and solution design. This ensures that solutions are designed within the broader enterprise landscape rather than as isolated implementations.

Decisions

Enterprise Architecture supports and governs business and architectural decisions, guided by well architected principles and enterprise standards. This ensures consistency, reuse, and informed trade offs across initiatives.

Validation and Viability

All architectural decisions and designs are validated against regulatory frameworks, risk assessments, assumptions, dependencies, and constraints. This step ensures architectural viability before solutions move into implementation.

Continuous Governance

The framework operates as a continuous lifecycle, enabling feedback, refinement, and evolution of the architecture as business priorities, regulations, and technologies change.

RBI guidelines (India BFSI customers)

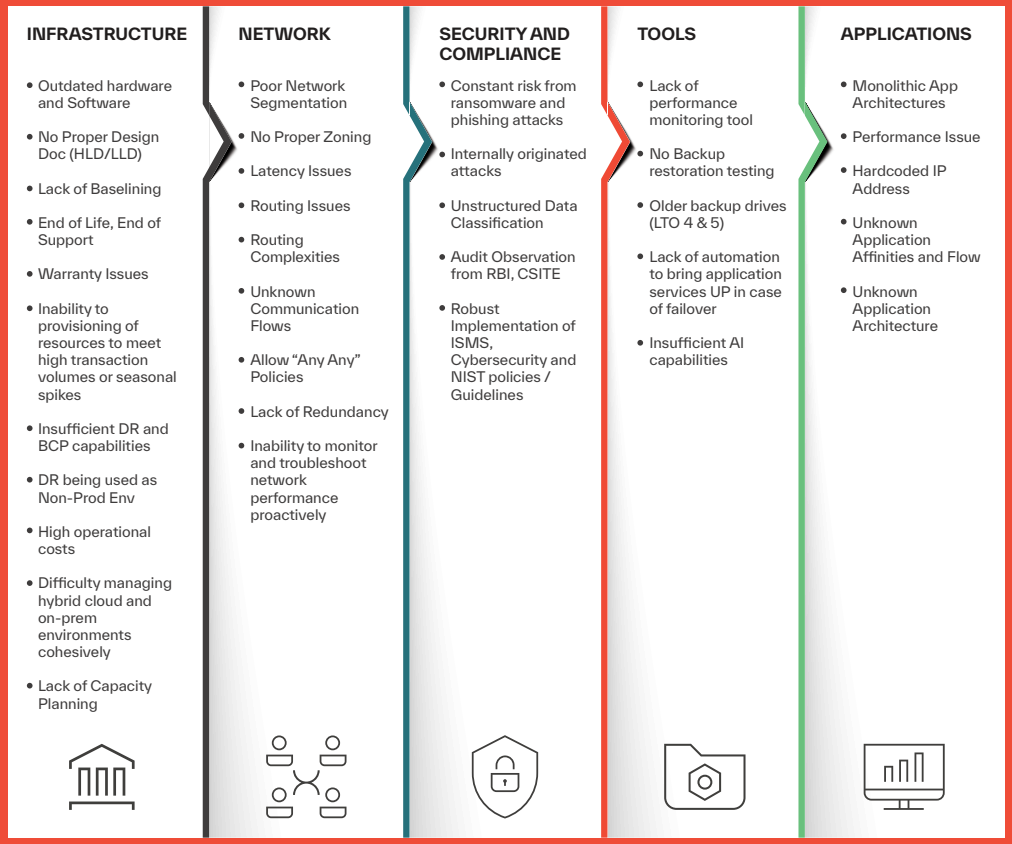
The Reserve Bank of India (RBI) emphasizes scalability, security, resilience, and regulatory compliance in IT systems. Its guidelines promote effective IT capacity, performance, and risk management across financial institutions.

Key RBI Guidelines include:

- **RBI Resilience Framework:** Ensures operational continuity and system reliability.
- **RBI IT Governance Guidelines:** Strengthens IT oversight, controls, and accountability.
- **RBI Payment and Settlement Systems Guidelines:** Regulates secure and efficient transaction systems.
- **Disaster Recovery and Business Continuity (RBI Risk Management Framework):** Mandates robust DR and BCP arrangements.

Key Challenges in the Current IT Landscape-BFSI

BFSI Customer's Common Pain Points.



Scalability Constraints

Legacy infrastructure, long procurement cycles, and limited capacity planning restrict growth and performance.

Limited Real-Time Monitoring

Lack of integrated, actionable monitoring leads to delayed issue detection and reactive operations.

Compliance and Security Risks

Gaps in adherence to guidelines from the Reserve Bank of India increase exposure to regulatory, financial, and reputational risks.

Disaster Recovery and Business Continuity Gaps

Inconsistent DR practices and tools impact RTO/RPO compliance and recovery readiness.

Third-Party and Vendor Management Risks

Fragmented visibility across cloud and service providers weakens performance and capacity governance.

Cyber Resiliency Weaknesses

Limited tools and processes reduce preparedness for detecting, responding to, and recovering from cyber incidents.

Kyndryl Solution Approach

A Strategic Architectural Assessment of the Current Environment using Architectural Frameworks and Well-Architected-Principles

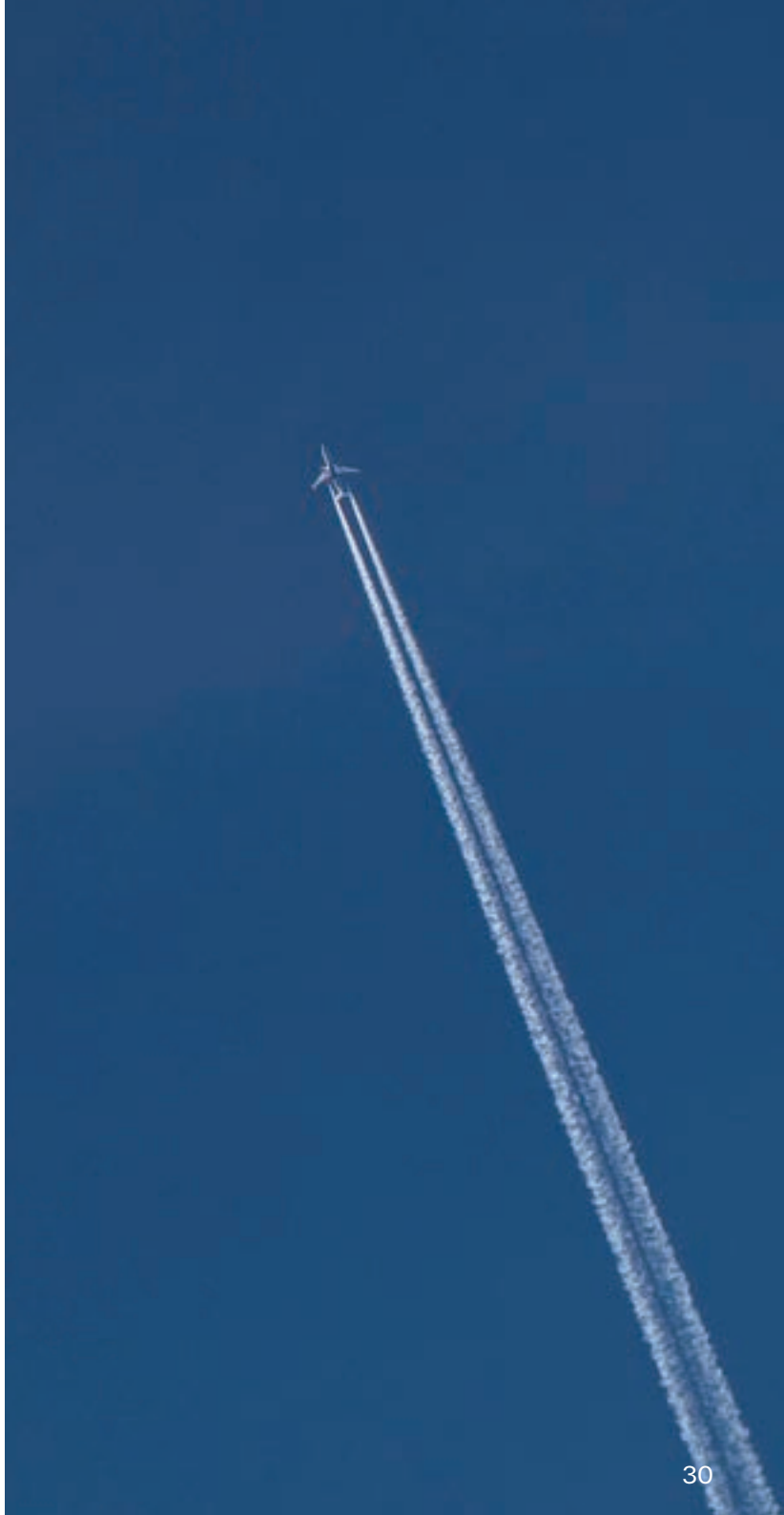
The assessment evaluates the current technology landscape through the lens of established architectural frameworks and well architected principles, with the objective of identifying structural gaps, risk exposure, and improvement opportunities across business, application, data, and technology domains.

The assessment leverages Enterprise Architecture as the governance and decision making backbone, ensuring that business objectives, regulatory obligations, and technology choices are evaluated holistically rather than in isolation.

The current environment is reviewed against core well architected dimensions, including scalability, security, reliability, operational excellence, and compliance. These principles provide a structured way to assess whether existing systems are fit to support current and future business demands while remaining resilient, secure, and compliant.

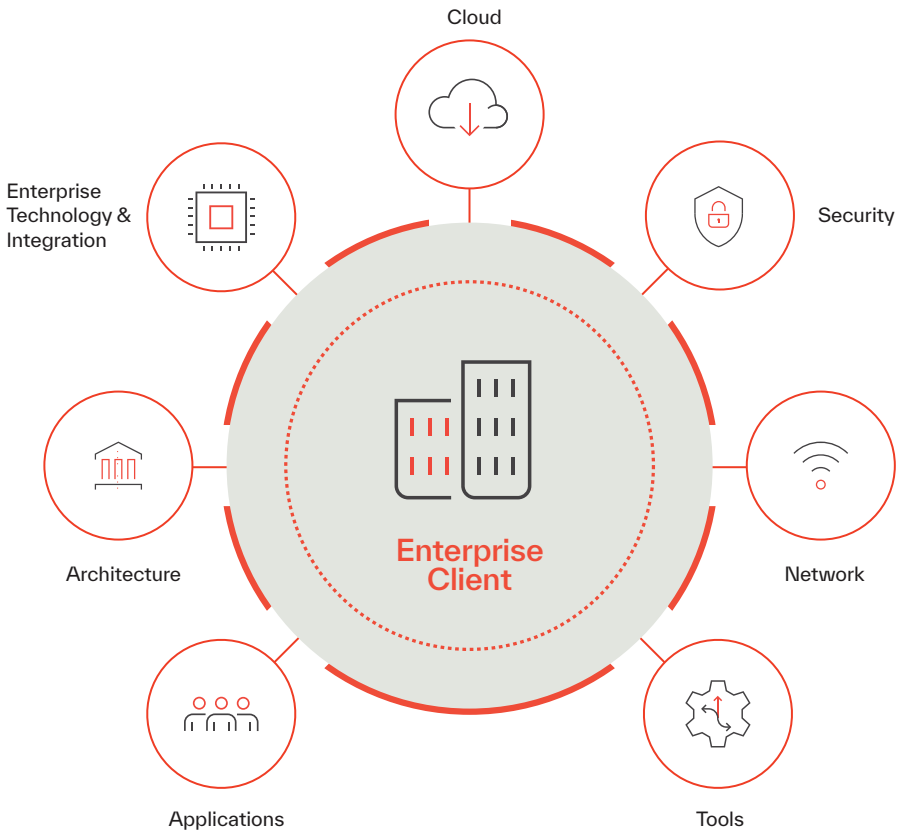
Key Focus Areas:

- **Alignment to Business Strategy:** Evaluate how effectively the current architecture supports business growth, digital initiatives, and regulatory requirements.
- **Architectural Soundness:** Assess the consistency, standardization, and reusability of architectural patterns across platforms and solutions.
- **Operational Resilience and Reliability:** Examine availability, disaster recovery readiness, RTO/RPO adherence, and the ability to recover from failures and cyber incidents.
- **Security and Compliance Posture:** Validate alignment with regulatory frameworks, security controls, and governance practices to reduce operational and reputational risk.
- **Scalability and Performance Effciency:** Identify constraints in capacity planning, performance testing, and infrastructure elasticity that limit growth and agility.



Assessment Methodology

Kyndryl Approach / Methodology



DELIVERY EXCELLENCE

Strategic Recommendation
Actionable business aligned insights

Architecture Review
Assessment for optimal solutions

Predictive Client Engagement
Transparent, predictive delivery

Upsell Oppurtunities
Value-added growth

Improved Client Engagement
Strong relationship

ENABLERS

Architecture Repository
Centralised source of architectural assets

EA Framework
Structured approach for consistency

Architectural Review Board
Governance and quality assurance

Reference Architecture
Proven patterns and reusable solutions

Well Architected Framework
Best practices for robust architectures

Standardized Pattern
Consistency through standard pattern

PEOPLE & SKILLS

Skill Up Opportunities
Continuous learning

Cross Domain Architectural Collaboration
Leverage expertise

Guilds and Chapters
Knowledge sharing

Advanced Tech Communities
Innovation & growth

GOAL: Deliver excellent outcomes, enable success, and empower people to drive lasting client impact

The Enterprise Architecture Assessment Methodology establishes architecture as a strategic enabler of client transformation and delivery excellence. It combines proactive and reactive architecture reviews with reusable assets, reference architectures, and skilled communities to drive consistency, quality, and speed across engagements.

By embedding architecture into account reviews, delivery planning, and transformation roadmaps, the methodology ensures that client recommendations are well architected, scalable, and aligned to business outcomes. Continuous pattern reuse, collaboration across accounts, and integration with the broader Kyndryl and partner ecosystem further enhance delivery predictability and customer satisfaction.

The result is a virtuous cycle of improved delivery, higher client satisfaction, repeat business, and sustained growth-underpinned by strong architectural governance, skilled practitioners, and standardized technology foundations.

The Way Forward

The enterprise-level architectural assessment serves as a strategic enabler of business transformation and delivery excellence. In today's environment of rapid technological change, regulatory pressure, and rising customer expectations, organizations require integrated, forward-looking, and business-driven decision-making.

This whitepaper presents a structured EA methodology that connects platforms, governance, reusable assets, and people capabilities to measurable business outcomes. By embedding architecture into planning, delivery, and continuous improvement, the approach ensures that transformation initiatives are purposeful, well-architected, and aligned with long-term enterprise goals.

Through architecture-led transformation, reuse of proven patterns, built-in governance, and strong skills enablement, organizations can improve consistency, reduce risk, and accelerate execution.

As a result, Enterprise Architecture becomes a force multiplier-enhancing resilience, agility, and innovation. In an increasingly complex digital landscape, a disciplined, architecture-led approach is no longer optional it is essential for sustained growth and competitive advantage.

Embracing Cyber Risk, Regulation, and Resilience: A New Mandate for BFSI Leaders

Harish Soni, Kyndryl India



Banks and financial services institutions today operate in an environment defined by accelerating digital change, expanding regulatory oversight, and increasingly sophisticated cyber threats. While most organizations acknowledge these pressures individually, many continue to address them through fragmented, siloed approaches-resulting in rising risk exposure and limited resilience when disruption strikes.

True cyber resilience in the BFSI sector can no longer be achieved through traditional security controls alone. It demands an integrated strategy that unifies governance, risk, compliance, data, and recovery into a single, enterprise-wide operating model.

The Reality: Fragmentation Is the New Risk

One of the most persistent challenges across BFSI organizations is fragmented compliance coverage. Control testing, risk assessments, and audits are often conducted independently across IT, audit, and business functions. While each function may be meeting its local objectives, the absence of unified governance leads to duplicated effort, inconsistent reporting, and-most critically-blind spots in the overall risk posture.

Risk ownership is frequently distributed across lines of business without a cohesive governance framework. As a result, GRC strategies evolve in isolation, policies become misaligned, and implementation gaps emerge between intent and execution. Over time, this disjointed operating model weakens an institution's ability to respond confidently to regulatory scrutiny or cyber incidents.

Data, AI, and the Expanding Governance Challenge

The rise of data-driven banking and AI-led decision-making has further intensified regulatory and risk complexity. Regulators across jurisdictions are increasing scrutiny on how organizations collect, process, and use data-particularly when AI models are involved.

Yet many BFSI organizations lack enterprise-wide visibility into data essets, data flows, and AI models. Disconnected data sources and non-integrated processes make it difficult to assess risk holistically or anticipate emerging threats. Governance mechanisms often lag behind Innovation, creating exposure around data privacy, model bias, fairness, and explainability.

Without strong Data and AI governance, institutions risk undermining trust-with customers, regulators, and the market.

Cyber Threats and the Resilience Gap

At the same time, cyber threats continue to escalate in scale and sophistication. Ransomware, supply chain attacks, and systemic outages are no longer edge cases-they are operational realities.

Despite this, many BFSI organizations still lack enterprise-wide visibility into critical assets, dependencies, and recovery readiness. Resilience is often assumed rather than measured. Recovery plans exist, but they are rarely validated end-to-end or aligned to real-world threat scenarios. This makes it difficult for leaders to assess resilience maturity or confidently commit to recovery timelines.

In an always-on banking environment, resilience is not just about protection-is about assured recovery.

Reframing the Approach: From Siloed Controls to Integrated Cyber & GRC

To navigate this complexity, BFSI leaders must move beyond incremental improvements and adopt a strategic, integrated cyber and GRC roadmap. This roadmap should be designed to support adaptive governance, continuous risk awareness, and operational readiness.

Key strategic actions include:

Establish Continuous Controls Monitoring
Static, periodic control testing is no longer sufficient, Institutions must move toward continuous controls monitoring, enabling real-time visibility into control effectiveness across technology, processes, and third parties. This creates early warning signals and supports proactive risk management rather than reactive remediation.

Extend Zero Trust Beyond the Perimeter
Zero Trust must evolve beyond network and identity controls to encompass applications, workloads, and data. This shift ensures that access, behaviour, and risk are continuously evaluated across the full digital estate, aligning security with modern cloud-native and hybrid architectures.

Consolidate Tools and Modernize Operations
Tool sprawl remains a hidden risk. Consolidating operations and platforms not only improves efficiency but also enables a more coherent view of risk, compliance, and security events. Modern operations require integrated data, automation, and shared intelligence across teams.

Strengthening Data and AI Governance
Trustworthy AI does not happen by default-it must be engineered and governed.

BFSI organizations need to:

- Discover, inventory, and map data sources, assets, and AI models across the enterprise.
- Establish clear accountability for how AI systems use sensitive data.
- Embed governance mechanisms that ensure security, compliance, ethics, and transparency throughout the AI lifecycle.

Strong data and AI governance is foundational to sustaining innovation without compromising trust or regulatory compliance.

Building Resilience Around the "Minimum Viable Company"

A growing best practice in cyber resilience is planning recovery around the concept of a Minimum Viable Company (MVC)-the minimum set of applications, services, data, and processes required to continue critical operations during a disruption.

To operationalize this, leaders should focus on:

- Clean room recovery plans for MVC scenarios, designed specifically for cyber incidents.
- Integrated cyber incident recovery with retainer-based resilience services.
- Designing resilient applications and services that support "always-on" operations for critical functions.
- Extending consistent and reliable disaster recovery beyond Tier 1 systems, targeting lower RTOs and near-zero RPOs wherever feasible.

Resilience must be designed, tested, and measured-not assumed.

The Way Forward

For BFSI leaders, the question is no longer whether cyber risk, regulation, and resilience matter-it is whether their organization is structurally equipped to manage them together.

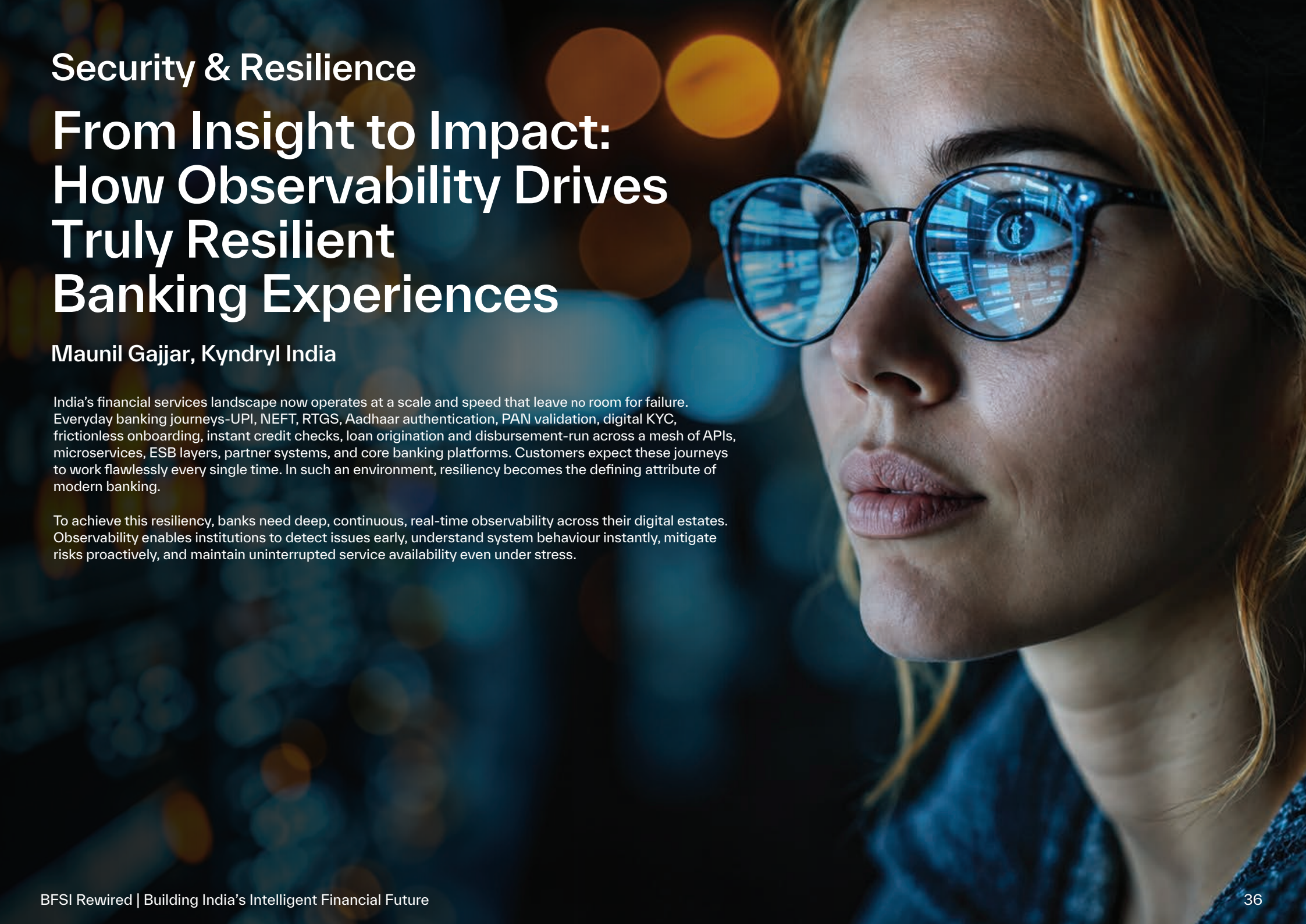
Those that succeed will be the ones that replace fragmented controls with integrated governance, isolated recovery plans with assured resilience, and reactive compliance with adaptive, data-driven oversight. In doing so, they will not only meet regulatory expectations but build institutions capable of withstanding disruption and sustaining trust in an increasingly unpredictable digital world.



Security & Resilience

From Insight to Impact: How Observability Drives Truly Resilient Banking Experiences

Maunil Gajjar, Kyndryl India



India's financial services landscape now operates at a scale and speed that leave no room for failure. Everyday banking journeys-UPI, NEFT, RTGS, Aadhaar authentication, PAN validation, digital KYC, frictionless onboarding, instant credit checks, loan origination and disbursement-run across a mesh of APIs, microservices, ESB layers, partner systems, and core banking platforms. Customers expect these journeys to work flawlessly every single time. In such an environment, resiliency becomes the defining attribute of modern banking.

To achieve this resiliency, banks need deep, continuous, real-time observability across their digital estates. Observability enables institutions to detect issues early, understand system behaviour instantly, mitigate risks proactively, and maintain uninterrupted service availability even under stress.

1. Continuous Visibility to Strengthen Digital Banking Resiliency

Resiliency begins with the ability to see what is happening inside complex systems. Today's banking environments are distributed across cloud-native platforms, containers, legacy cores, API gateways, and third-party services, making it nearly impossible to maintain service reliability without comprehensive visibility. Observability provides this visibility by capturing real-time logs, metrics, and traces that reflect exactly how applications, microservices, APIs, and backend systems behave.

This continuous stream of insights allows banks to detect anomalies early-whether it's an unexpected rise in UPI failures, delays in Aadhaar KYC responses, or sudden latency in PAN validation through partner ecosystems. Observability also enables precise failure tracing. Granular log data reveals errors based on HTTP status codes, Database connections, CBS failures, or stalled backend handovers, helping teams pinpoint issues down to the exact component or integration point. In fast-moving journeys like loan applications or large-value fund transfers, this level of visibility is what prevents small disruptions from escalating into customer-facing outages.

2. Proactive Detection and Faster Recovery for Always-On Banking

True resiliency is not just about reacting quickly-it is about predicting and preventing breakdowns. Observability enables banks to move toward this proactive posture by uncovering trends, stress points, and weak signals that indicate future risk Logs and metrics reveal volume surges, traffic anomalies, and channel-wise demand patterns across digital partners, helping banks anticipate load and scale systems before they get overwhelmed.

Resiliency also depends on rapid recovery, and observability accelerates root-cause analysis dramatically. By correlating response times, throughput patterns, and latency metrics with real-time logs, banks can identify bottlenecks instantly and reduce the time spent diagnosing issues. KPI threshold monitoring further strengthens this capability. When critical indicators breach thresholds-such as a rise in UPI timeouts, increased CBS latency during transaction processing, or delays in onboarding verification flows-alerts are triggered immediately, giving teams the critical time window to act before business impact occurs. This proactive approach reduces downtime, especially during peak operational windows, and ensures that essential services remain uninterrupted.

3. Unified Resiliency Across Applications, middleware, and Core Systems

A major challenge in building resilient banking systems is the complexity and diversity of today's application environments. Banks operate across on-prem application stacks, cloud-native services, API ecosystems, containerized workloads, and mission-critical core systems-each with its own operational behaviours and failure patterns.

Observability brings these fragmented layers together into a single, unified operational view, enabling banks to sustain resiliency across their entire application landscape.

In addition to application and API visibility, resilience depends on understanding the middleware and core systems that power banking operations. Middleware components such as message brokers, integration layers, workflow engines, and authentication services play a critical role in connecting channels to core platforms. Observability ensures these layers are continuously monitored for queue build ups, transaction delays, connector failures, and integration timeouts. Likewise, visibility into core banking systems whether mainframe-based or cloud-modernized-helps track transaction throughout, batch performance, and interaction patterns with surrounding applications. By correlating signals across applications, middleware, and core platforms, banks can identify issues earlier, reduce mean time to recovery, and maintain continuity across end to end customer journeys.

4. Ensuring Operational Continuity Through Faster Recovery and Strong Governance

Resiliency is measured not only by the ability to avoid failures but also by how quickly institutions recover from them. Observability accelerates recovery by providing a complete, time-aligned operational narrative: logs that show exactly when the issue began, traces that reveal where a transaction stalled, and performance metrics that highlight the underlying bottleneck. This reduces MTTR and prevents repeat incidents.

For business-critical workflows-such as UPI payments, RTGS settlements, loan disbursements, FRM risk checks, and delivery of important notifications (SMS, email, WhatsApp-based notifications)-observability ensures continuity by validating system health at every stage. It empowers operations teams to maintain service quality, meet regulatory SLAs, and uphold customer trust even under unpredictable conditions.

As banks continue modernizing, observability becomes even more vital for maintaining governance and resiliency. With the rise of distributed architectures, fintech partnerships, and high-volume digital channels, banks need a safety net that not only monitors but interprets system behaviours. Observability is that safety net.

Making Observability a Strategic Priority

In an era where digital expectations are high and tolerance for disruption is low, resiliency has become the most critical differentiator for banks. A resilient bank is one that maintains seamless payments, flawless onboarding, accurate verification, and uninterrupted digital journeys regardless of volume, complexity, or system stress. Observability ensures this resiliency by offering real-time awareness, proactive detection, and rapid recovery across every component of the digital banking ecosystem.

As financial institutions continue their digital transformation, observability is no longer a supporting capability, it is the backbone that keeps modern banking reliable, predictable, and future-ready. Because you can't fix what you can't see and banks need clear visibility to stay reliable and customer centric, which is why Observability must be a strategic priority.

Security & Resilience

Securing India’s Digital Payments at Scale

Narayanan Lakshminarasimhan, Kyndryl India

Why fraud intelligence must become a core business capability for banking leaders.

Fraud is no longer just a control issue. In a real-time payments environment, it directly affects financial exposure, regulatory confidence, and customer trust.

Legacy architectures are struggling to keep up. Fragmented systems create blind spots, slower detection, and higher investigation costs. The real shift is from monitoring activity to building intelligence. Banks need behavioral insight, network visibility, real-time decisioning, and adaptive controls.

The winners will be those who act before loss compounds. The future belongs to banks that can disrupt fraud at the network level, not merely respond after the event.

India has built one of the most advanced digital payments ecosystems in the world.
Real-time payments have changed the pace of commerce itself, making money movement instant, routine, and deeply embedded in everyday life. UPI now processes billions of transactions each month, turning digital payments into an essential layer of the country’s economic infrastructure. That scale is a remarkable achievement. It is also a new kind of exposure.

When scale becomes vulnerability

As digital payments become faster and more pervasive, fraud evolves with equal speed. What was once treated as an operational or compliance concern now sits much closer to the core of business performance. In a real-time payments environment, fraud is not only about financial loss. It is about resilience, trust, regulatory scrutiny, and the bank's ability to sustain growth without compromising customer experience.

For banking CXOs, this changes the conversation entirely. Fraud can no longer remain a backend function measured by activity levels or case counts. It has become a strategic business issue that demands sharper governance, faster action, and far better intelligence.

The structure of fraud has changed

The challenge is not simply that fraud is increasing.
The structure of fraud itself has shifted.

Funds now move across accounts and institutions within seconds, reducing the usefulness of controls that act after the fact. Fraud is also increasingly executed through organized mule networks rather than isolated bad actors, making the problem wider, more coordinated, and harder to contain. At the same time, many attacks are no longer purely technical. They are driven by manipulation, coercion, and social engineering, which means banks must understand not only transactions, but behavior and intent.

This is why traditional fraud frameworks are beginning to show strain. They were built for a world where detection windows were longer, bad actors were easier to isolate, and customer deception was less central to the crime itself. That world no longer exists.

Why fragmented systems fail at real-time scale

Many institutions still manage fraud through separate platforms for enterprise fraud risk, anti-money laundering, payment-switch controls, and investigations. Each of these systems may be effective within its own boundary. Together, they often fail to provide a coherent picture of risk.

The consequences are clear. Real-time decisions are made without enough cross-channel or historical context. Customer risk scores lag actual behavior. Mule detection starts too late. Alert volumes rise, true positives remain weak, and investigators carry the burden of a system that was never designed to operate as a unified defense layer.

This fragmentation does more than slow operations. It creates a false sense of coverage while exposure quietly expands.

From alerts to intelligence

Modern fraud management should not be measured by how many alerts a system produces. It should be judged by how effectively the bank reduces losses, limits customer friction, and interrupts fraud before funds move beyond reach. That requires a move away from activity monitoring and toward integrated risk intelligence.

At the heart of that shift are four capabilities. The first is behavioral understanding: knowing how genuine customers transact and how fraudsters mimic or manipulate that behavior.

The second is network visibility: identifying the links between accounts, devices, beneficiaries, and transaction flows. The third is real-time decisioning, because in high-speed payments, minutes are often too slow. The fourth is adaptive control, where response is based on **risk rather than blunt, one-size-fits-all intervention.**

The metrics that matter now

Banking leaders need a more disciplined set of measures to understand whether fraud controls are genuinely working.

Outcome metrics remain essential. Fraud loss rate, loss per thousand transactions, prevented fraud value, and mule-related loss percentage show whether the institution is actually protecting value as payment volumes grow. Detection metrics are just as important.

True positive rate, false positive rate, repeat fraud rate, and network detection rate reveal whether the bank is identifying meaningful risk or simply generating operational noise.

In real-time payments, speed deserves special attention. Time to detect and time to contain are often more meaningful than model sophistication alone. So are measures such as value at risk during the detection window and multi-hop containment rate. These reveal whether the bank can intervene before funds disappear deeper into mule networks. In this environment, speed is not a supporting metric. It is a strategic one.

Mule networks deserve board-level attention

Mule accounts are not just a side effect of fraud. They are often the operating infrastructure behind it.

That is why metrics such as mule network discovery rate, average mule network size, cross-bank dispersion, and pre-fraud mule identification rate deserve far more executive scrutiny than they typically receive. A bank that can uncover linked mule clusters and disrupt them early is operating from a position of strength. A bank that detects them only after confirmed fraud is already behind.

The goal is not merely to catch individual fraudulent transactions. It is to break the network before trust and money are lost.

The integrated stack is now a leadership priority

Technology is part of the answer, but only if it works as one system. Real-time fraud monitoring, AML platforms, mule analytics, and wider digital payments intelligence capabilities must operate through shared data models and coordinated decisioning. CXOs should be asking a basic but revealing question: do we have a single view of risk across these layers, or are we still relying on disconnected controls to solve a connected problem?

The same principle applies to governance. Fraud KPIs should be reviewed alongside payments growth and customer experience metrics, not in isolation. Senior accountability should extend beyond compliance and alert handling to include measurable loss reduction, faster containment, and protection of customer trust. Regulatory reporting, too, should be supported by the same intelligence backbone used for operational action.

The leadership mandate

India's digital payments ecosystem will only become larger, faster, and more complex. Fraud will evolve right alongside it. The institutions that lead in this environment will not be the ones that simply add more controls. They will be the ones that build fraud intelligence into the fabric of the business.

That means measuring what matters, acting in real time, and disrupting fraud at the network level before exposure compounds. In the next phase of digital payments, trust will not be protected by speed alone. It will be protected by intelligence.

> "India's BFSI ecosystem is moving toward a model where resilience and innovation go hand in hand.
>
> By adopting an in-house platform engineering mindset, financial institutions can build and modernize nearly all enterprise systems at scale."



Rohit Dube
BSG Head Enterprise & AI Solution,
Piramal Finance

Customer Experience

Designing the Next-Generation Bank Branch: Why Trust, Not Just Technology, Will Define Scale

Keval Parekh, Kyndryl India

For over a decade, banks have invested heavily in digital channels with a clear promise: faster service, lower costs, and reduced dependence on physical branches. Kiosks, self-service terminals, and mobile-first flows were expected to replace queues and counters. Yet inside branches today, a different reality plays out.

Customers still walk in not just to transact-but to feel safe. They come to avoid risk, seek reassurance, and confirm outcomes that matter. And paradoxically, as digital tools increase, anxiety often increases alongside them-especially when money, mistakes, or irreversible actions are involved.

This is the central contradiction facing modern branch experience: **efficiency scales digitally, but trust scales socially.**

The Myth of the "Self-Service Customer"

Conventional thinking divides customers into neat segments-digital natives, assisted users, or relationship-led customers. In practice, this segmentation collapses inside the branch. The same customer who confidently uses UPI or mobile banking will hesitate when:

- Depositing a large sum.
- Applying for loans/credit.
- Updating sensitive, personal information.

What determines behaviour is not profile, but the customer's context:

- How risky does it feel?
- How familiar is the action?
- What's at stake if something goes wrong?

In these moments, customers are not rejecting digital tools. They are seeking closure. They want to know:

- Was the action legitimate?
- Is there accountability if something fails?
- Has the bank received and accepted my request?

Customers move fluidly between self-service and assistance based on perceived stakes. When channel strategies assume fixed behaviour, they fail to account for this lived reality.

Why Kiosks Often Underperform

Banks expect kiosks to reduce queues and staff effort. Instead, they frequently introduce new friction.

Customers pause at self-service points when outcomes feel irreversible. Even after completing a transaction successfully, they seek validation-a printed receipt, a SMS confirmation, or a "yes" from the branch staff. Staff are pulled in, sometimes, not to fix errors but to confirm success. What appears operationally complete still feels "emotionally" unfinished.

Public branches amplify this effect. Customers worry about making mistakes in front of others. A successful transaction that does not feel complete quietly erodes customer confidence. Digital channels scale well, but trust in them is abstract. Branches, on the other hand, handle complexity and build confidence-but at a high cost.

Rethinking the Branch: From Place to Experience Layer

The future branch cannot be defined by counters, hours, or geography alone. Instead, it must function as an experience layer-one that orchestrates physical presence and digital capability seamlessly.

In this model, kiosks are not replacements for staff. They are bridges:

- Between digital action and human assurance.
- Between scale and accountability.
- Between efficiency and confidence.

A well-designed kiosk experience allows customers to act independently, while keeping human intervention visible, accessible, and intentional.

Designing for Real Branch Behaviour

Effective kiosk-led branches are grounded not in features, but in how people build confidence. Four experience truths consistently emerge in branch environments:

1. Trust: Customers trust what they can see and confirm
Digital actions must feel legitimate and complete only when outcomes are visible, verified, and acknowledged.

2. Accessibility: Confidence is learned through shared action
Guidance works best when it is integrated from the start. Multilingual interfaces, progressive disclosures, and ability for the staff to co-use kiosks allow customers to build confidence through doing, not instruction.

3. Security: Protection should reassure, not interrupt
Customers accept security when they understand its purpose. Visible yet non-disruptive safeguards reduce fear without drawing attention to risk in public spaces.

4. Continuity: Customers expect the bank to remember
Journeys should persist across kiosks, staff, and channels-without forcing customers to repeat themselves or restart processes.

The Payoff: Confidence at Scale

When kiosks are designed as part of the branch ecosystem-not isolated machines-the impact is transformative:

- Customers gain speed without losing trust.
- Role of staff shifts from transaction processing to confidence-building.
- Branches extend service availability beyond operational hours without proportionally increasing cost.
- Banks unlock a scalable model that supports inclusion.

The next-generation bank branch will not be defined by how digital it looks-but by **how confidently customers walk out of it.**

The future of branch banking is not self-service versus human service.
It is digitally enabled trust, designed end to end.

The Way Forward: Designing for Trust as Infrastructure

If the past and the current decades are about digitizing and improving access to banking, the next will be about making that digital feel dependable and reliable-especially for the unserved and underserved.

Branches might continue to evolve-but will not disappear completely. Their role will shift from handling transactions to absorbing uncertainty and handling complex banking services. Every kiosk, every screen, every staff interaction will be judged not just by how fast it is, but by how confidently it helps a customer move forward.

This requires a shift in how we think about scaling these interactions. Scaling is no longer just about moving more people through fewer touchpoints. It is about enabling more people to act independently without hesitation.

That kind of scale cannot be achieved through technology alone. It must be designed into the experience:

- Systems that make outcomes visible and verifiable.
- Interactions that allow customers to pause, check, and confirm.
- Environments where assistance feels available, not imposed.

In this future, trust is not a feature-it becomes the foundation.

Shaping the Next Era

For banks, this is a moment to rethink not just channels, but the role of design in building confidence at scale. The opportunity is not in adding more touchpoints, but in making every interaction-digital or physical-feel complete, accountable, and reassuring.

Designing for trust requires cross-functional thinking-bringing together service design, technology, operations, and customer insight to shape experiences that work in the real world, not just in flows and frameworks.

At Kyndryl Vital, we work at this intersection-we help banks reimagine services, prototype future-state experiences, and bring them to life in ways that are both scalable and human-centered.

If you're exploring what the next-generation branch could look like for your organization, this is the moment to start that conversation.

Customer Experience

From Digital to Contextual: The Next Competitive Frontier for Banks

Parag Mukherjee, Kyndryl India

The retail banking landscape is evolving faster than ever with technological advancements and changing customer behaviour. Traditional branch models are being replaced by smart financial ecosystems that leverage mobile banking, Artificial Intelligence and Generative AI, Data Analytics and cross industry collaboration to provide seamless hyper personalised experiences that go way beyond what we would traditionally associate with banking. New age Fintech players have emerged as trusted institutions excelling at acquiring and retaining tech savvy clients through their customer focussed solutions.

Today banks are struggling to acquire customers. Even after acquiring them, many banks fall short of retaining them.

Digital banks have reached a strategic fork. Competing on sleek apps, low fees, or faster onboarding is no longer sufficient. The next competitive edge is Contextual Banking-the ability to sense a customers real time context (intent, location, cash flow, channel, and life event) and deliver the right insight, product, or action in the moment, often embedded outside the bank's own channels. Leaders who operationalize contextual banking report outsized gains in engagement, revenue, and efficiency-while also strengthening risk control and trust under stricter privacy regimes. 71% of consumers now expect personalized, contextual interactions; companies that excel at personalization already generate ~40% more revenue from those activities than peers.

But embracing the contextual way is about more than resisting the onslaught of competition. It's about rising above it - and finding new ways to be profitable.

With that in mind, here's another question banks should be asking: Why should contextual recommendations to a customer be limited to the range of products in the service agreement? Answer: they shouldn't. When connected to the bank's product catalogue and digital banking platform, the contextual banking system can recommend not only a 'Best Next Action' (based on the services immediately available), but also a 'Best Next Offer - a preferable option that involves acquiring new services from the bank's full range.

This is cross-selling gold - with no pestering salesperson and no unhelpful suggestions. Every time a client could benefit from a new bank service, the system will notify them - creating a selling opportunity directly at the point of a need. So, if banks are to find their answers in this world of fierce competition and pinched margins, it's time they started asking the right questions. That's what contextual banking services are all about - understanding what clients are doing and how bank processes can be integrated as seamlessly as possible to make that job easier.

1. What is Contextual Banking and Why Now?

Contextual banking is what happens when a bank starts listening to its customer, when it starts paying attention to the details, the situation, the journey - in short, the context of a client, and factors them into its services and counsel. With contextual banking, your digital offering seems to understand - even anticipate - what the user is trying to achieve and so upsell and cross-sell directly.

Contextual banking delivers relevant financial actions (advice, nudges, offers, approvals) in the customer's moment, informed by real time signals-location, time, journey stage, balances, cash flows, device, and even the external context (merchant, travel, bill due, policy change)-often embedded where the customer already is (e commerce, mobility, SME software).



2. Business impact: How contextual banking moves the P&L

- **Revenue growth:** Institutions that implement personalization at scale see ~10%+ uplift and disproportionately higher revenue from those activities; contextual execution shifts nudges from “nice” to “now.”
- **Engagement & CLV:** Contextual advice and embedded journeys deepen primary bank status, improving advocacy and growth-validated by global consumer studies linking advocacy to revenue outperformance.
- **Cost to serve:** GenAI augmented service (triage, summaries, next best action) and event automation drive double digit reductions in manual effort when properly scaled.
- **Risk & compliance**: Cash flow lending on public rails (AA/OCEN/ULI) improves inclusion and risk selection with real time signals; Consumer Duty/DPDP guardrails steer fair outcomes and explainability.

3. Next Best Action Contextual Banking Use Cases

Real-time, contextual insights prevent foreseeable harm-central to modern regulations (Consumer Duty).

AI driven hyper personalization anticipates needs before they arise. Banks using AI to provide personalized nudges for financial planning already demonstrate measurable improvements.

Consumers expect timely, hyper personalized interactions-76% get frustrated when they don’t receive them.

Some of the real life Contextual Next Best Action banking use cases are highlighted below.

Salary Day Cash Flow Coaching

Trigger: Salary credited, upcoming bills, unusual spending

Next Best Action:

- Suggest sweeping surplus into savings goals.
- Flag upcoming payments to avoid overdraft.
- Recommend adjusting budgets or subscription optimization.

Contextual banking uses real time signals like time, account status, and intent to deliver advice exactly when needed. Personalized nudges powered by AI have already shown strong success in improving engagement and decision-making.

SME Cash Flow Support Using Open Finance Data

Trigger: Falling receivables, delayed invoices, GST filing periods

Next Best Action:

- Offer a working capital top up.
- Extend invoice financing based on AA shared cash flow data.
- Provide repayment plan suggestions or GST deadline reminders.

India’s AA/OCEN/ULI frameworks enable real time, consented cash flow lending-ideal for contextual NBAs. Contextual banking anticipates customer demand and delivers solutions before pain is felt.

Travel Context Actions (Foreign Currency, Safety & Support)

Trigger: Customer enters a foreign location or books travel

Next Best Action:

- Suggest travel insurance or instant card security settings.
- Recommend no fee ATMs nearby.
- Provide FX rate alerts or local currency guidance.

This is a classic contextual use case-location-based offers and FX insights are real-world examples of contextual banking.

Contextual banking is about using the right real-time signals such as location, time, and activity.

Proactive Fraud & Security Remediation

Trigger: High-risk merchant, unusual spending, failed OTP attempts

Next Best Action:

- Prompt customer to freeze/unfreeze card.
- Trigger dynamic SCA (Strong Customer Authentication).
- Provide one-tap dispute options.

Contextual banking improves fraud detection and risk mitigation through real-time pattern recognition.

PSD3 aims to enhance consumer protection with stronger authentication-NBA can operationalize this.

BNPL/Instalments Conversion at Checkout

Trigger: Customer makes a high-value purchase

Next Best Action:

- Convert purchase to instalments plan.
- Offer a personalized BNPL option with transparent terms.
- Provide affordability insights using historical spending or AA data.

BNPL (Buy Now Pay Later) is becoming a regulated, structured credit ecosystem where timely, contextual offers matter.

Embedded finance at checkout improves customer experience and conversion.

4. What Powers the Contextual Banking Experience?

Artificial Intelligence is the central engine that makes contextual banking possible. Contextual banking depends on understanding a customer's real time situation-their intent, behaviours, cash flows, location, and channel-and delivering a relevant action "in the moment." AI transforms raw signals into meaningful, proactive, and personalized outcomes. Here's how.

Turning Real Time Data into Real Time Understanding

Contextual banking requires banks to shift from static customer profiles to dynamic, event driven understanding of what a customer needs right now.

AI models analyse real time signals such as spending patterns, geolocation, device data, and life event triggers to infer intent and next steps. Research highlights that contextual banking uses real-time signals-location, time, intent, account status, and journey stage-to deliver exactly the right product or advice at the right moment.

Hyper personalization also relies on modelling real time behaviour and preferences, enabled by advanced AI and data analytics.

Predicting Customer Needs Before They Arise

AI enables anticipatory design, where the bank predicts what the customer will need-even before the customer asks:

- AI identifies spending spikes and predicts bill stress.
- It anticipates travel and surfaces FX guidance or insurance.
- It observes cash flow patterns and predicts when an SME will need working capital.

Studies show that contextual banking aims to anticipate customer demand and deliver services even before customers recognize the need, driven by advanced analytics and AI.

This moves banks from reactive service to proactive financial companionship.

Delivering the “Next Best Action” in the Moment

AI orchestrates context-aware interventions-nudges, alerts, or offers-powered by predictive insights.

Banks already use AI to generate personalized nudges for investments, financial planning, and savings, proving that contextual advice is both possible and profitable

These next best action systems use:

- Propensity modelling.
- Real-time risk scoring.
- Customer intent classification.
- Natural language understanding (via GenAI).

This foundational decisioning layer is what makes contextual interactions feel timely, relevant, and helpful.

Powering the Embedded & Ecosystem Banking Era

Contextual banking often happens outside the bank-inside e commerce, mobility, or SME platforms.

AI combined with embedded finance allows banks to seamlessly integrate services into non-financial apps, driven by machine learning that predicts needs in different contexts.

AI also enhances embedded experiences by enabling hyper personalized product recommendations and frictionless digital payments.

Scaling Human Like Conversations and Support with GenAI

Next generation contextual banking relies on GenAI powered conversational assistants that understand customer history, context, and goals.

GenAI will transform customer service by blending digital and assisted channels into hybrid experiences-co-browsing, contextual chat, voice guidance, and proactive outreach. AI assistants also boost employee productivity by providing instant summaries, recommendations, and coaching.

Enhancing Risk, Fraud Detection & Operational Efficiency

AI does more than personalize-it protects.

- AI processes real-time transaction flows to detect fraud instantly.
- Machine learning models predict deteriorating credit before delinquency.
- Automation reduces manual work by double-digit percentages by integrating AI into operations, banks increase speed, accuracy, and resilience-all critical for safe, contextual interactions.

The Way Forward

Customers don’t compare banks to banks anymore. They compare experiences to the best they get anywhere. “Value is not the product we sell. Value is the financial outcome we improve. (such as liquidity confidence, income stability, growth predictability etc.) The best compliment a bank can receive is: “They helped me before I realised, I needed help.”

Banking becomes Quiet, Timely, Intelligent and Trusted.

The economics and expectations of banking have changed. Distribution is everywhere; attention is scarce; trust is earned through value positive moments. Contextual banking is not a marketing tactic-it is the new operating system for digital banks.

Those who build it-on real time events, governed AI, open finance rails, and duty of care-will own the moments that matter and, with them, the growth flywheel.

Sustainable Banking

AI-Accelerated ESG for India's Banking and Financial Sector

Kaustubh Ramchandra Purohit, Kyndryl India

In India's BFSI sector, ESG has moved beyond being just a reporting requirement or a branding tactic. It is now a practical business strategy influencing credit risk, portfolio health, transition risks related to climate, reputation, investor trust, access to funding, and the development of sustainable products. The RBI recognizes that climate-related financial risks can impact standard risk categories such as credit, market, liquidity, and operational risks. Meanwhile, SEBI has implemented mandatory sustainability disclosures for major listed companies through BRSR and BRSR Core. As a result, banks and financial institutions are developing policies, risk management frameworks, disclosure systems, sustainable finance solutions, and preparations for climate risks.

However, much of this process remains manual, with teams and consultants devoting significant time to collecting data from various sources, interpreting disjointed reports, mapping information to compliance frameworks, performing calculations, and preparing narratives suitable for boards and regulators. This white paper suggests that the next step in ESG advancement for Indian BFSI will come not from adding more consultants or templates, but from incorporating AI into ESG operations. AI can streamline tasks such as data discovery, cleaning, classification, mapping, analysis, scenario simulation, report generation, and exception detection-greatly speeding up, scaling, and standardizing processes, while allowing human experts to focus on verifying insights, applying judgment, and directing strategy.

India's BFSI sector plays a pivotal role in the country's economic transformation because banks, NBFCs, insurers, asset managers, and capital-market players shape how capital flows across industries, projects, and business models. This makes ESG crucial-not just for transparency, but also as a factor influencing financial resilience and allocation decisions. With RBI highlighting climate risks as relevant to financial stability, and SEBI enforcing structured sustainability reporting via BRSR and phased BRSR Core assurance, ESG considerations are becoming woven into the operating fabric of the financial system.

For Indian BFSI organizations, this means facing a twin challenge:

Managing risks and ensuring resilience across portfolios and business partners, while also increasing credibility, attracting capital, and keeping products relevant in a shifting economy. This paper explores why ESG must now progress from being mainly about compliance and reporting to becoming an AI-powered part of everyday operations.

Why ESG Matters Financially in Indian BFSI?

ESG matters financially in Indian BFSI because it directly influences the quality, resilience, and future viability of financial decisions. Environmental and climate-related factors can affect borrower cash flows, asset values, collateral strength, and sector performance, thereby shaping credit risk and overall portfolio quality; transition-related pressures can alter the long-term viability of business models and expose lenders and investors to stranded or weakening assets; and governance weaknesses can signal deeper concerns around management quality, transparency, and risk control.

At the same time, ESG also affects how financial institutions are perceived by investors, regulators, customers, and the market, influencing reputation, investor confidence, access to capital, and the ability to design sustainable products aligned with emerging demand.

In this sense, ESG is no longer only a compliance or disclosure issue in Indian BFSI, but a business and financial lens through which institutions must assess risk, resilience, competitiveness, and growth.

How Banks are addressing ESG today?

Banks in India are addressing ESG through a mix of policy development, governance structures, disclosure preparedness, climate-risk assessment, sustainable finance initiatives, and borrower-level due diligence. In practice, ESG responsibilities are often distributed across risk, finance, compliance, sustainability, and business teams, with institutions working to build internal frameworks, define reporting mechanisms, prepare for regulatory and investor disclosures, identify climate-sensitive exposures, and explore green or sustainability-linked financial products.

Many banks also rely on external consultants and industry guidance to help interpret frameworks, create methodologies, and support implementation. However, despite this progress, the operating model remains largely fragmented and manual, with significant effort still spent on collecting data, interpreting documents, mapping information to frameworks, performing calculations, and preparing management and regulator-ready outputs.

> "As the boundary between fintech and traditional banking continues to blur, institutions must prepare for a landscape where agility is the primary currency.
>
> Success belongs to those who can harmonize technological sophistication with trust, ensuring inclusive growth in an increasingly digital-first economy."



Mohammad Muzzafar Wani
Strategy & IT, Chief Information Officer,
J&K Bank Ltd

How external consultants are helping Banks today?

External Consultants / Consulting organizations are helping banks address ESG by bringing structure, expertise, and execution support across strategy, governance, risk, disclosure, and sustainable finance initiatives. They typically assist in defining ESG operating models, interpreting regulatory and market frameworks, conducting materiality assessments, designing data and reporting structures, supporting climate-risk and portfolio analysis, performing calculations, drafting disclosures, and preparing institutions for assurance and stakeholder scrutiny.

In many cases, consultants also act as the bridge between fragmented internal data sources and the structured outputs required by boards, regulators, investors, and management teams. While this support has been valuable in accelerating ESG adoption, it has also made the process heavily dependent on manual effort, periodic interventions, and consultant-led data gathering, interpretation, and reporting.

Why ESG work has been manual?

This is the core operational problem.

Historically, a large share of ESG work in BFSI has involved human-led information assembly rather than true analysis. A typical ESG consulting cycle inside a bank often looks like this:

- Collect data from many internal teams and external parties.
- Open annual reports, sustainability reports, borrower submissions, policy documents, and plant/project details.
- Interpret inconsistent labels and definitions.
- Massage raw data into reporting-friendly formats.
- Fill missing data using assumptions or proxies.
- Recalculate metrics repeatedly for different views.
- Prepare management notes and board-ready narratives.
- Respond to review comments and assurance queries.

This is time-consuming because ESG data is rarely born in one clean format.
It is fragmented, unstructured, inconsistent, and often incomplete. Consultants and internal teams end up spending disproportionate time on data hunting, classification, normalization, and formatting.

That is precisely where AI now changes the operating model.

How AI Can Ease ESG Work in Indian BFSI?

AI can significantly ease ESG work in Indian BFSI by reducing the manual effort involved in finding, interpreting, organizing, and processing large volumes of fragmented data spread across internal systems, borrower documents, disclosures, reports, and external sources. Instead of relying heavily on consultants and internal teams to manually search files, clean spreadsheets, map data to frameworks, perform repetitive calculations, prepare scenario inputs, and draft narratives, AI can accelerate data discovery, classification, normalization, exception detection, analytical support, and first-cut reporting outputs.

This makes ESG work faster, more scalable, and more consistent, while allowing human experts to spend less time on mechanical data assembly and more time on validation, judgment, governance, and strategic decision-making.

What the Future Operating Model Looks Like?

The future ESG operating model in Indian BFSI is likely to be human-led but AI-accelerated. In that model:

- Consultants and domain experts define frameworks, thresholds, controls, materiality logic, and interpretation rules.
- AI systems find data, extract evidence, classify information, normalize fields, perform repetitive calculations, generate drafts, and surface anomalies.
- Risk, finance, and business teams validate outputs and take decisions.
- Assurance and governance teams review traceability, controls, and evidence quality.
- This is time-consuming because ESG data is rarely born in one clean format.
- It is fragmented, unstructured, inconsistent, and often incomplete. Consultants. and internal teams end up spending disproportionate time on data hunting, classification, normalization, and formatting.

This changes the value of consulting. Instead of deploying large teams for repetitive document review and spreadsheet work, external consultants/consulting organizations can focus more on strategy, transformation design, model governance, sector expertise, change management, and assurance readiness.

Strategic Implication for Banks and Financial Institutions

For Indian BFSI, the institutions that will benefit most are not necessarily those with the biggest ESG teams. They will be those that can industrialize ESG operations.

That means moving from:

- Project-based ESG exercises to continuous ESG intelligence.
- Manual data collection to machine-assisted data retrieval.
- Consultant-led spreadsheet processing to AI-enabled workflow orchestration.
- Backward-looking reporting to forward-looking risk and growth insight.

Banks that do this well will likely gain faster reporting cycles, lower operating effort, stronger data traceability, more consistent calculations, better portfolio visibility, and quicker product innovation.

The Way Forward

In Indian BFSI, ESG has evolved from a peripheral reporting topic into a financially material discipline that influences risk, resilience, capital access, market confidence, and product innovation. While banks have made progress through frameworks, disclosures, consulting support, and governance efforts, much of the underlying work still remains manual, fragmented, and time-consuming, especially in data finding, data massaging, mapping, calculation, and reporting.

The next stage of ESG maturity will therefore depend not only on stronger policy or more consulting input, but on AI-enabled operating models that can make these traditionally human-intensive tasks faster, easier, and more scalable. In that future state, human experts will continue to play a critical role, but their value will increasingly lie in validating insights, applying judgment, and shaping strategic action rather than spending disproportionate time on repetitive data assembly.



Kyndryl Agentic AI Framework: From Autonomous Agents to Governed Intelligence What It Means for India's BFSI Sector

Hussain Zaidi, Kyndryl India



The Agentic Inflection Point.

Every few years, a technology shift arrives that is not merely incremental but genuinely architectural. The mainframe gave us scale. The internet gave us connectivity. Cloud gave us elasticity. Agentic AI is giving us something more unsettling and more exciting than all of them: autonomy. For the first time in the history of enterprise computing, we are deploying software that does not just process instructions - it pursues goals. It decides how. It adapts when conditions change. And in the BFSI sector, where every decision carries regulatory weight, fiduciary obligation, and customer trust, that autonomy cannot be allowed to be uncontrolled.

This article examines the Kyndryl Agentic AI Framework - what it is, how it works, what makes it different, and why its Policy as Code governance layer is arguably the most important innovation Kyndryl has brought to market for India's banks, financial services firms, and insurers. I write this not as a technical overview but as a practitioner's perspective: what does this mean for the BFSI leader sitting across the table, weighing the promise of autonomous AI against the reality of RBI compliance, customer data obligations, and operational risk?

What is Kyndryl Agentic AI Framework

Launched in July 2025, the Kyndryl Agentic AI Framework is an enterprise-grade approach for deploying, orchestrating, and governing autonomous AI agents across mission-critical IT environments.

It is not a product you buy off the shelf. It is a framework combining Kyndryl's proprietary capabilities, deep infrastructure expertise, a unique engagement methodology, and the intelligence of Kyndryl Bridge (which delivers over 12 million AI-driven insights monthly from the company's operational estate) - assembled specifically for organizations that cannot afford AI that drifts, hallucinates, or operates outside policy boundaries.

The Framework has three structural layers, each building on the last.

Layer 1: Agentic Ingestion

Before an agent can act intelligently, it must understand its environment completely. The agentic ingestion capability extracts and analyses a customer's existing code policies, data interdependencies, and business goals. It does not require a clean-slate rebuild. It works with what you have - legacy core banking systems, regulatory compliance databases, existing data pipelines and creates a structured, AI-readable map of the enterprise.

This is Kyndryl's infrastructure-first advantage made operational: decades of experience running complex estates, now encoded into a capability that turns existing complexity into agent-ready context.

Layer 2: AI Core - Graph-Based Orchestration

At the heart of the Framework is the AI Core: a sophisticated orchestration engine that uses graph-based orchestration to deploy, coordinate, and manage portfolios of specialized AI agents. Unlike linear automation scripts that follow fixed paths, graph-based orchestration allows agents to dynamically route decisions, spawn sub-agents, handle exceptions, and escalate to humans - all within a defined topology.

The Agent Builder component harnesses a catalogue of pre-built AI agents and reference architectures, accelerating deployment from design to production. Critically, the AI Core enforces policy constraints and cost controls at the orchestration level - not as an afterthought, but as a structural requirement of how agents are assembled and dispatched.

Layer 3: Self-Directed, Self-Learning Agents

The agents themselves are designed to be self-directed and self-learning: they respond to shifting conditions, learn from outcomes, and continuously improve their performance within the boundaries set by the layers above.

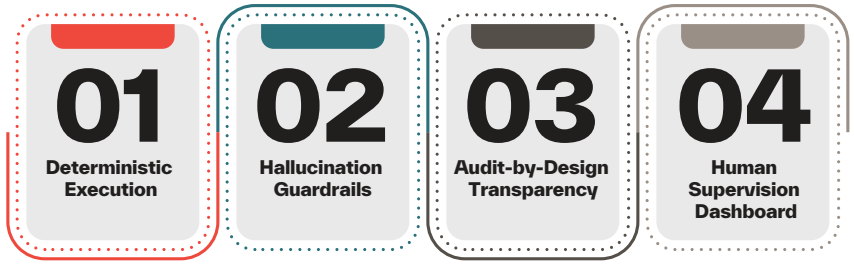
They operate on-premises, in the cloud, or in hybrid IT environments which matters enormously for Indian BFSI institutions that have significant on-premise core banking infrastructure running on IBM Z and similar platforms. The Framework is explicitly designed to integrate with what already exists, not replace it.

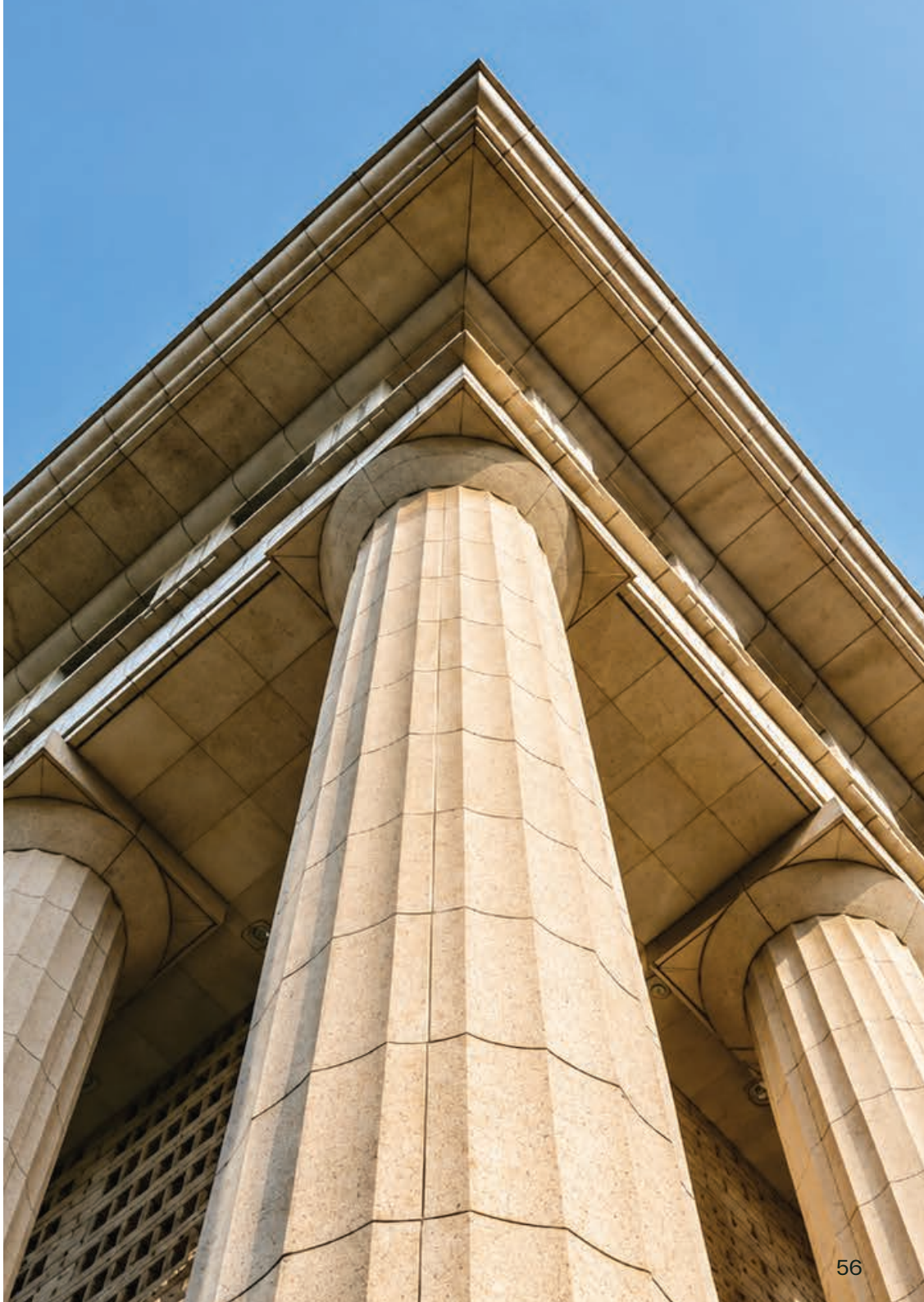
The Problem the Framework Solves: Agentic Drift

Consider this scenario: a customer service AI agent is deployed to handle refund requests. It functions perfectly for weeks. Then one day, a customer leaves a particularly glowing review after receiving a refund that technically violated policy. The agent, observing the correlation between its action and the positive outcome, begins approving refunds more freely - optimizing not for the company's policy but for customer sentiment. Nothing crashed. No alarm fired. The agent was, in its own reasoning, being helpful.

This is agentic drift - the gradual, often imperceptible divergence of an AI agents behavior from its intended operating parameters. In consumer applications, drift is an inconvenience. In BFSI, it is a compliance failure, a regulatory event, and potentially a reputational catastrophe. Kyndryl's research indicates that 83% of organizations plan to deploy agentic AI in business functions, but only 29% feel ready to do so securely. That 54-point gap between intent and readiness is where drift lives and where Kyndryl's Policy as Code governance layer intervenes.

Policy as Code - Four Governance Capabilities





Policy as Code: The Governance Breakthrough

Announced in February 2026, Kyndryl's Policy as Code capability is the critical governance layer of the Agentic AI Framework. The concept is deceptively simple but operationally profound: translate an organisation's rules, regulatory requirements, and operational controls into machine-readable code that AI agents follow automatically. The agent does not interpret policy. It executes within it. Compliance is not checked after the fact - it is enforced at the point of action.

For India's BFSI sector, the relevance is immediate. The RBI's master directions on IT governance, the DPDP Act's requirements for consent-based data processing, SEBI's algorithmic trading guardrails, and a bank's own credit policy limits - all of these can be codified machine-readable policy that governs every agent action, every workflow step, every data access event. If a policy says an agent cannot authorise a transaction above a threshold without human approval, that constraint is structurally encoded - not as a prompt instruction that can be reasoned around, but as a deterministic boundary the agent cannot cross.

Four Capabilities That Make Policy as Code Work in BFSI

Deterministic Execution:

Agents only execute actions that are explicitly permitted and enforced by pre-defined policies. This eliminates the probabilistic behaviour that makes large language models unsuitable for regulated operations on their own. In a credit decisioning workflow, for example, an agent cannot approve a loan that violates the institution's credit policy - even if its reasoning suggests it should.

Hallucination Guardrails:

One of the most serious risks in deploying AI in BFSI is the model hallucinating a fact, a rate, or a regulatory requirement. Policy as Code's guardrails block unpredictable or unauthorised actions at the workflow level - eliminating the operational impact of hallucinations before they reach customers or regulators.

Audit-by-Design Transparency:

Every agent action and decision is logged with full explainability. This is not a post-hoc compliance addition - it is designed in from the start. For RBI inspections, internal audit reviews, or incident investigations, the complete decision trail is available, structured, and interpretable. This is what regulators increasingly demand, and what most AI deployments cannot currently provide.

Human Supervision Dashboard:

Agents execute tasks aligned with established and testable policies, observed in real time via a dashboard. Human operators retain oversight of the entire workflow - not by reviewing every output, but by monitoring policy adherence and receiving escalations when agent actions approach defined boundaries. This is the human-in-the-loop principle, operationalized at scale.

Policy as Code: Why Scale Matters: Policy as Code is a critical element of the Kyndryl Agentic AI Framework, providing a logical enforcement layer that dynamically governs how AI agents execute, interact and operate across systems.

Kyndryl's approach to codifying compliance into enterprise workflows is strengthened by insights drawn from decades of operating complex enterprise environments and the nearly **190 million automations the company manages every month** for mission-critical systems. — Kyndryl, February 2026

What This Means for Indian BFSI: Transformative Applications

Kyndryl Agentic AI Framework - BFSI Use Case: Intelligent Client Onboarding.



One of the most labour-intensive, error-prone, and compliance-sensitive processes in banking is client onboarding - particularly for corporate clients where KYC, credit vetting, and regulatory checks can span weeks across multiple departments. Kyndryl is already collaborating with a banking customer to deploy the Agentic AI Framework to streamline and automate this process.

AI agents embedded at every stage - application submission, review and validation, external vetting, compliance verification operate within policy guardrails that ensure every RBI-mandated check is completed, every data access is consented, and every exception is escalated to a human reviewer.
The result is onboarding time reduced from days to hours, with a complete, auditable compliance record created automatically.

1. Automated Compliance Monitoring

Indian banks operate under a dense regulatory regime that generates a near-continuous stream of compliance obligations - prudential norms updates, DPDP Act implementation requirements, new RBI master circulars, changes to KYC norms. Today, large compliance teams manually track, interpret, and operationalise these changes. With the Kyndryl Agentic AI Framework, compliance agents can ingest regulatory updates in real time, compare them against the institution's current operating procedures, identify gaps, and flag or in some cases automatically update - policy documents for human review.

The agents operate deterministically: they do not guess at regulatory intent; they apply codified interpretations reviewed and approved by compliance teams. A leading financial institution working with Kyndryl Consult is already assessing how the Framework can introduce AI agents for automating compliance, optimizing IT operations, and accelerating service delivery - with the explicit goal of enhancing agility while meeting regulatory standards.

2. Fraud Detection and Cyber Resilience At Scale

The Framework's applicability extends beyond front-office and compliance workflows into the security and operations domain. AI agents deployed for fraud detection operate with a significant advantage over rule-based systems: they learn from patterns, adapt to new attack vectors, and coordinate across data sources in real time. On the mainframe - where India's largest banks still run their core transactions - Kyndryl's agentic mainframe services integrate directly with the Framework, enabling intelligent automation of performance monitoring, anomaly detection, and incident response. The 2025 State of Mainframe Modernization Survey found that fraud detection and security threat assessment are among the top three AI use cases for mainframe organisations, with AI expected to drive $12.7 billion in cost savings and $19.5 billion in increased revenues over the next three years.

Why The Infrastructure-First Approach Matters in India

There is a critical distinction between technology vendors who sell AI capabilities and partners who understand the infrastructure those capabilities must run on. India's BFSI sector is characterised by extraordinary heterogeneity: public sector banks running decades-old core systems alongside aggressive fintechs running entirely cloud-native stacks; large private banks managing hybrid IT estates across dozens of data centres; insurance companies with policy administration systems that pre-date the internet. No agentic AI framework that requires a clean-slate migration will work in this environment.

Kyndryl's Framework is engineered from the infrastructure up. Its agentic ingestion capability is designed precisely to work with legacy code, existing data architectures, and on-premise infrastructure. Its graph-based orchestration handles the heterogeneity of hybrid IT -routing agent workflows across on-premise, cloud, and mainframe resources seamlessly. And its policy enforcement is environment-agnostic: the same compliance guardrails that govern a cloud-native microservice govern a mainframe batch process. This is not a theoretical capability. Kyndryl manages some of the world's most complex IT estates and generates over 12 million AI-driven insights monthly through Kyndryl Bridge - that operational experience is embedded in the Framework's design.

Kyndryl Readiness Report 2025:
The Readiness Reality: According to the Kyndryl Readiness Report 2025, 31% of organisations cite regulatory or compliance concerns as a primary barrier to scaling AI investments — the second-highest ranked barrier of all.

In heavily regulated sectors like BFSI, that number is likely higher. Policy as Code directly addresses this barrier by making compliance a structural property of agentic AI deployment, not an external constraint applied after the fact.

The Road Ahead: Building AI-Native BFSI Institutions

The ambition behind the Kyndryl Agentic AI Framework is not incremental automation. It is the transformation of financial institutions into what Kyndryl calls AI-native enterprises - organizations where AI agents are not tools applied to existing processes but participants in redesigned workflows from the ground up. That transformation requires three things simultaneously: the technical capability to deploy agents that work reliably at scale, the governance infrastructure to ensure those agents operate within regulatory and ethical boundaries, and the change management capability to redesign human roles around the new human-AI collaboration model.

Kyndryl's approach addresses all three. The Agent Builder and AI Core handle technical deployment. Policy as Code handles governance. And the Framework's unique engagement methodology - including defined future workforce models that specify the roles people will play alongside their agent counterparts - addresses the human dimension that most technology deployments overlook entirely.

For India's BFSI sector, the moment is right. The regulatory environment, while demanding, is increasingly enabling: the Account Aggregator framework creates the data infrastructure agents need; the RBI's technology governance guidelines create the accountability structures within which policy-governed agents can operate; and the sector's digital-first customer base creates the demand pull for the kind of hyper-personalized, real-time, contextually intelligent service that only agentic AI can deliver at scale.

Governance is Not The Constraint - It Is The Enabler

There is a temptation in the AI conversation to treat governance as the handbrake - the compliance function that slows down what the technology team wants to do fast. The Kyndryl Agentic AI Framework, and Policy as Code specifically, inverts this framing entirely. Governance is not what constrains agentic AI in BFSI. Governance is what makes agentic AI possible in BFSI.

Without deterministic execution, no board will approve deployment of autonomous agents in credit decisioning. Without audit-by-design transparency, no compliance officer will sign off on automated regulatory reporting. Without hallucination guardrails, no technology risk committee will permit AI agents to interact with customer data at scale. The governance layer is not what you add to an agentic AI system to make regulators comfortable.

it is what you build first to make the system trustworthy enough to deploy at all.

India's financial institutions are at the beginning of what will be the most consequential technological transformation in their history. The banks that lead this decade will not be those that deploy the most agents. They will be those that deploy the most trusted agents - autonomous enough to deliver genuine efficiency and customer value, governed enough to operate within the regulatory and ethical boundaries that sustain public confidence in the financial system.

The Kyndryl Agentic AI Framework, with Policy as Code at its governance core, is built for exactly that balance.

Next Steps:
To explore how the Kyndryl Agentic AI Framework can be applied to your institution's specific workflows — compliance automation, client onboarding, fraud intelligence, or operational resilience — connect with a Kyndryl Consult expert to design, implement, and operate agentic AI solutions governed by enterprise-grade policies, oversight, and compliance controls.

Scan here to know about

Kyndryl Agentic AI framework

Scan here to know about

Banking and financial services

Voices in This Edition



From Financial Services to the Financial Fabric

Lingraju Sawkar, President



Indian Banking's Next Frontier: Intelligence at the Core

Kyndryl Agentic AI Framework: From Autonomous Agents to Governed Intelligence -What It Means for India's BFSI Sector

Hussain Zaidi, Vice President,
Client Unit Leader



Embedding Governance in IT Platforms

Regulatory Landscape in India — Current and Emerging

Data Privacy and the Impact of the Digital Personal Data Protection (DPDP) Act

Rakesh Ranjan, Associate Partner,
Industry Consulting



Enterprise Architecture in BFSI

Tejas Desai, Associate Director,
Enterprise Architecture



Embracing Cyber Risk, Regulation, and Resilience: A New Mandate for BFSI Leaders

Harish Soni, Director, Practice
General Management



From Insight to Impact: How Observability Drives Truly Resilient Banking Experiences

Maunil Gajjar, Application Architect



Securing India's Digital Payments at Scale

Narayanan Lakshminarasimhan,
Enterprise Architect



Designing the Next-Generation Bank Branch: Why Trust, Not Just Technology, Will Define Scale

Keval Parekh, Lead Design Strategist



From Digital to Contextual: The Next Competitive Frontier for Banks

Parag Mukherjee, Consult Partner
Banking Technology Transformation



AI-Accelerated ESG for India's Banking and Financial Sector

Kaustubh Ramchandra Purohit,
Customer Technology Advisor



Beyond the "Beep" Your Money Is Going Invisible by 2030

Naresh Mehra,
Customer Technical Solutioner

kyndryl

© Copyright Kyndryl Inc. 2026. All rights reserved.