Swaminathan J: Issues and challenges in banking supervision in the digital era

Speech by Mr Swaminathan J, Deputy Governor of the Reserve Bank of India, at the Third Annual Global Conference of the College of Supervisors, "Adapting the regulation and supervision to the digital age", Mumbai, 9 January 2026.

* * *

Respected Governor;

Deputy Governor, Shri S C Murmu;

Chairman, Academic Council, College of Supervisors, Shri Arijit Basu; and members of the Academic Council of CoS

Director, CoS, Shri R. Subramanian;

Distinguished speakers, panellists and Managing Directors & CEOs of Regulated Entities;

My fellow colleagues from RBI, Ladies and Gentlemen.

A very good morning to all of you. It is a pleasure to be with you today at the third edition of the annual global conference of the College of Supervisors of the Reserve Bank of India.

As we all know, banking is becoming more digital, more connected, and more complex. So, I will use this opportunity to take this one step further and speak about what "Supervision in the digital age" really means on the ground, for us and the supervised entities. How our questions change? How our engagement will change, and what we expect boards and management to demonstrate-before the next incident tests the system!

What changes on the ground for supervisors?

Let me start with a simple thought. For decades, supervisors were trained to read balance sheets and inspect processes. We still do that. But today, a bank can look perfectly healthy on paper and still be one incident away from severe disruption. The reason is that the centre of gravity is shifting from the "branch and product" to the "pipes and code". In other words, stability now depends as much on operational resilience, data integrity, and third-party dependencies as much it does on capital and liquidity.

Therefore I would like to dwell upon how has the risk landscape changed in the digital age:

a. The first is speed. In the digital world, both growth and stress can travel faster. Customer acquisition can be exponential, but so can misinformation, panic, and outflows. Risks that used to take weeks to build can now crystallise in hours. This

means supervisory feedback loops must tighten, with early triggers, faster follow-up, and clear escalation.

b. Secondly, concentration and interdependence. Many institutions may rely on the same core service providers, cloud platforms, payment rails, data vendors, and cybersecurity tools. This creates a new form of common exposure. It is not always visible in traditional financial ratios, but it is very real. For supervision, we need to map dependencies more actively and assess concentration risk at the ecosystem level, not only at the individual institution level.

c. Third is the growing role of algorithms. AI and machine learning are entering credit underwriting, fraud detection, customer service, treasury, and even internal control functions. This improves efficiency but also raises new questions of accountability, explainability, and fairness. Supervisors need to be able to ask, and entities need to be able to answer, a simple question: who owns the outcome when a model drives a decision?

d. The fourth is an expanded threat surface and cyber risk. Digital banking increases points of entry, and the adversary is no longer a random hacker. It is often organised, well-funded, and persistent. Even when a bank's internal controls are strong, a weakness at a vendor, a partner, or a common technology component can spill over. Resilience and recovery must be treated as core capabilities.

e. Lastly and perhaps most importantly, there are conduct risks in a digital wrapper. Digital lending, embedded finance, and platform-based distribution have significantly improved access and convenience. But we have also seen risks of mis-selling, opaque charges, aggressive recovery practices, and data misuse. In a digital environment, customer harm can quickly become a confidence issue, and that can quickly transform into a liquidity issue.

How supervision must respond: principles before tools

Let me now turn to the supervisory response. We certainly need better tools, but we must start with a few fundamental principles that keeps supervision grounded even as technology evolves.

The first is technology-neutral, risk-based supervision. We should regulate and supervise activities and risks, not technology brand names. Innovation will keep changing. Our objectives do not and there is no real replacement to human judgement.

The second is proportionality. Not every institution has the same complexity, systemic footprint, or technology maturity. The supervisory approach must be risk-based, calibrated and proportional, but without lowering expectations for basic controls, such as cybersecurity hygiene, data protection, and governance.

The third is clear accountability. Digital systems can diffuse responsibility between bank, vendor, fintech partner, and so on and so forth. The supervisory approach must be clear: the supervised entity remains accountable for activities conducted in its name and on its rails.

The fourth principle is forward-looking supervision. In a fast-changing environment, backwards-looking compliance checks are necessary but not sufficient. We have to be able to spot weak signals early, test resilience before incidents occur, and intervene before vulnerabilities become events.

New Supervisory Focus Areas

These principles are not new. What is new is the supervisory mindset we need around them. Supervision must shift from periodic snapshots to continuous awareness. It also needs to move beyond a single institution and take a sharper view of its ecosystem. And finally, we need to move from asking only "did you comply?" to also asking "can you withstand stress, recover quickly, and protect customers when things go wrong?"

Let me translate that mindset into four supervisory focus areas that are becoming central in the digital age:

i. operational resilience and cyber readiness,

ii. ecosystem and third-party dependencies,

iii. governance of data, models and AI, and

iv. technology-enabled, continuous supervision, including better use of SupTech and analytics.

Operational resilience and cyber readiness

The first shift is in how we view operational disruptions. In the past, operational risk was often treated as a support function issue. In the digital world, it can become the main event. A few hours of outage, a serious cyber incident, or a breakdown at a key service provider can impair critical services.

This calls for deeper engagement with boards and senior management on cyber governance, crisis playbooks, recovery capability, and learning from near-misses. It also means simulations that test decision-making under pressure, not just documentation.

Ecosystem and third-party dependencies

The second focus area is the ecosystem around the supervised entity. Critical functions may be hosted by cloud providers, technology vendors, payment intermediaries, outsourced service centres, fintech partners, and data service providers. Collectively, the system can become exposed to a small number of common points of failure.

The cross-border element adds another layer. Many providers operate globally, and incidents do not respect jurisdictional lines. The global IT outage in July 2024 is a useful reminder. The lesson is not about any one firm, but about how quickly third-party incidents can transmit disruption at scale, including to well-run institutions. This calls for near real-time cooperation among supervisors.

Governance of data, models, and AI

The third focus area is the rise of data-driven decision-making, including AI. From a supervisory standpoint, the question is not whether a bank uses AI. The question is whether it can demonstrate governance and accountability around its use.

Two issues deserve particular attention. One is reliance on vendor models and embedded tools, in which the institution may use the output without fully understanding the underlying engine. The second is fairness and unintended exclusion, where data proxies can produce outcomes that appear efficient but are unacceptable. Governance is what allows innovation to scale safely.

Technology enabled continuous supervision

The fourth focus area is the supervisory transformation itself. If banking is becoming always-on, supervision cannot remain episodic. This requires on-site and off-site teams to work more closely together, to pick up early signals and for faster follow-up.

SupTech can help supervisors identify patterns early, detect anomalies, and focus attention where it matters most. But data quality and data governance remain critically important. With better data quality and right analytics, supervisors can increasingly connect dots across silos.

A sharper customer lens: grievance redress as an early warning indicator

Before I conclude, let me add one more point: customer service and grievance redress.

In a digital environment, a weak grievance system is not a minor irritation. It is often an early warning. From a supervisory angle, we need to look not only at whether a bank has a grievance framework, but at how it performs. Are complaints resolved on time? Do institutions identify root causes and close them, or do they only manage closures on paper? Do boards see a clear dashboard of complaint trends, repeat failures, and customer pain points? And, is there a proactive and swift remediation?

A mature digital financial system does not have zero complaints. Instead, it learns and fixes quickly, and customers can get fair outcomes without running from pillar to post.

Conclusion

Let me conclude by summing up what the digital age means for supervised entities and their supervisors.

For supervised entities, three messages are important.

i. First, compliance cannot be treated as a quarter-end activity. With faster cycles, banks will need stronger operational discipline and data governance throughout the year. When an anomaly is flagged, the ability to explain it and fix it quickly becomes a marker of control maturity.

ii. Second, third-party management must be treated as risk management. Institutions will need better oversight of partners, clearer accountability for incidents, and contracts that support audit, access, and resilience. The regulated entity cannot outsource responsibility.

iii. Third, as AI and analytics become more embedded, institutions should be prepared for more intensive supervisory questions on model risk, explainability, and fairness.

For supervisors, the bar is also rising. We need to remain rooted in the basics while also becoming more familiar with new risk areas. That means building the right mix of skills, including cyber, IT, data, and model expertise, alongside core prudential judgement.

This is where the role of College of Supervisors becomes central. The College is not only about training programmes. It is about building a shared supervisory language, practical comfort through casework and simulations, and the confidence to ask the right questions in new areas.

The College also has a broader role as a platform for peer learning, particularly with supervisors from the Global South. Many jurisdictions are navigating similar challenges: rapid digitalisation, first-time customers, platform-based delivery, and fast-changing threat landscapes. Sharing practical experience on what works and what does not is one of the quickest ways to raise supervisory effectiveness.

Finally, capacity building is not a one-time effort. Technology and business models will continue to evolve. Threat actors will keep adapting. Our training and supervisory methods must continue to grow as well.

Let me conclude. In the digital era, supervision must remain prudent but also become more vigilant, more ecosystem-aware, and more outcome-focused. The intent is not to impede innovation. Instead, it is to ensure that innovation rests on trust, resilience, and customer fairness.

I am confident that the deliberations in this conference will help us sharpen our thinking on these issues. I wish you all a productive conference, and I look forward to the discussions. Thank you. Jai Hind.