“India Needs to Build Forward-Looking GRC Frameworks with AI Defence”

Mohammad Saad,
VP, Operational Risk Management
Banking & Finance Sector Expert

“Strengthen Tech Defences Through Automation and Shared Intelligence”

Intro: As India’s financial sector races toward AI-led transformation, are its governance and audit systems truly ready for the risks ahead? With 66% of CAEs flagging emerging tech and cybersecurity as top threats, and GenAI promising 46% productivity gains by 2030, the stakes are rising fast. Can banks build cyber-resilient, transparent, multi-vendor, and ethically governed AI systems before innovation outpaces oversight? **Mohammad Saad, Operational Risk Management** expert answers these and more in a deep conversation with **Mahima Sharma** of **Indiastat**. This week our exclusive read on **Socio-economic Voices**.

MS: A survey found 66% of Chief Audit Executives (CAEs) in India list emerging tech (AI/ML/bots) and cybersecurity as the top governance risks. How should Indian banks and NBFCs restructure their GRC frameworks to address this large proportion of emerging-tech risk?

Mr. Saad: To manage emerging technology risks, Banks and NBFCs in India must enhance their GRC (Governance, Risk and Compliance) frameworks so these systems can identify threats early and respond rapidly, ensuring risks are effectively mitigated. Technology-driven risks evolve quickly, which means that solutions should be rooted in a forward-looking strategy rather than reactive measures.

Financial institutions should harness the capabilities of AI and ML to address emerging tech threats. Emphasis must be placed on automation, given that manual checks often depend on human effort and may not keep pace with risks that change faster than any other risk type.

AI is an excellent tool for proactively detecting threats before they become critical. Automated controls provide a stronger defense, as they outperform manual controls, which tend to be slower and less reliable against fast-moving technological risks.

Organisations must also have a resilient Enterprise Risk Management Framework that places technology risk at the forefront. For long-term resilience and security, banks and NBFCs in India should aim for a caber-resilient, technology-driven GRC model. This means using AI to actively defend and assess risk, continually benchmark against regulatory requirements and embedding security throughout every layer of digital operations in the financial sector.

MS: According to an EY report, generative AI (GenAI) could drive productivity gains of up to ~46% in Indian banking operations by 2030. What risk-management and governance controls must India’s banking sector put in

place to harness this productivity uplift while maintaining stability?

Mr. Saad: Generative AI (GenAI) can drive significant productivity gains for organisations, but it also introduces additional risks that require strong governance and control mechanisms for early detection and remediation. It can significantly benefit the organisations by automating repetitive tasks, enabling new innovations & enhancing productivity. Studies show GenAI adoption can increase employee productivity by over 60%, translating into substantial time savings and cost reductions.

However, GenAI also introduces new threats such as misinformation, data privacy concerns and potential misuse through generative content. To effectively manage these risks organisations must establish a robust governance framework that includes comprehensive controls to continuously monitor GenAI outputs, safeguard data security and ensure strict compliance with regulatory requirements.

Early detection systems powered by AI can recognise abnormal patterns to prevent misuse and safeguard against developing vulnerabilities. By combining AI-driven defense with comprehensive policies, organisations can harness the benefits of GenAI while mitigating associated risks responsibly.

MS: What strategies should India's banking industry adopt to mitigate systemic risk arising from reliance on a small set of AI/cloud providers or models?

Mr. Saad: Banking and financial institutions must develop a comprehensive resilience strategy to address the risks posed by dependence on a limited number of AI and cloud service providers or models. This strategy should focus on building a strong ecosystem that balances the advantages of innovative AI technologies with the imperative to mitigate systemic risks and maintain resilient operations in compliance with regulatory standards.

A key element is adopting a multi-vendor strategy. This reduces single points of failure by diversifying dependencies across various service providers and exploring a broad range of AI models. This approach ensures operational continuity even if one provider faces disruptions.

Institutions should invest in in-house research and cultivate innovation sandboxes that foster experimentation and development of proprietary capabilities. Equally important is encouraging continuous training and upskilling of employees to build strong internal expertise for managing evolving technologies effectively.

Developing a strategic approach toward the adoption of new technologies, combined with establishing strong governance mechanisms for continuous monitoring, auditing and accountability of AI models, will enable banks to maintain trust, security and compliance throughout their AI lifecycle.

MS: What audit, transparency and vendor-governance controls should India's financial institutions embed when deploying AI systems for risk and compliance?

Mr Saad: Financial institutions need to keep strong audit, transparency and vendor-governance controls in place when using AI systems. This helps them spot and fix risks that come up during AI deployment.

AI brings several kinds of risks like errors, bias, security gaps and privacy breaches. The data used to train AI models might be incomplete, biased or even tampered with, which can lead to unfair or unethical results. Because many AI systems work like a "black box," it's hard to explain their decisions or audit how they work. They're also open to attacks like data poisoning, which can corrupt the model.

Sometimes AI behaves unpredictably or produces wrong (“hallucinated”) information, creating operational problems. On top of that, using third-party data or tools can expose institutions to supply-chain risks. If governance isn’t transparent, these issues can quickly grow, leading to serious operational failures and violations of compliance rules.

The Reserve Bank of India (RBI) has recently published the Framework for Responsible and Ethical Enablement of Artificial Intelligence (FREE-AI). Financial institutions should refer to this and implement it to ensure compliance and mitigate risks inherent in AI systems.

Audit Controls

- The RBI’s FREE-AI framework requires regular and independent audits.
- These audits should match the level of risk and the sensitivity of each AI use case.
- The focus should be on finding bias, checking fairness and verifying accuracy.
- They should also review explainability and security at every stage of the AI lifecycle.
- Continuous monitoring is imperative to catch any drop in performance or unusual behaviour.
- This helps keep the AI model accountable.

Transparency Controls

- FREE-AI requires clear communication about how AI is being used.
- Institutions must share details about model limits, privacy measures and governance steps.
- They should make sure regulators and stakeholders can understand how the AI works.
- Consumer protection must be ensured through complaint and grievance systems.
- The board of the institution must take responsibility and review AI reports regularly.

Vendor-Governance Controls

- RBI stresses strict checks on vendors who provide AI solutions.
- This includes verifying compliance, privacy, risk management and ethical AI practices.
- Contracts must clearly mention audit rights, incident reporting and alignment with regulations.
- Institutions should keep watch over all third-party AI systems.
- They must make sure vendors follow RBI’s standards to avoid external risks.

MS: How can banks and NBFCs scale AI-driven fraud solutions across India while ensuring governance, legal/regulatory compliance and avoidance of unintended harms?

Mr. Saad: Banks and NBFCs can scale AI-driven fraud solutions by integrating advanced technologies and aligning their operational frameworks to handle huge transaction volumes, data-heavy sources and evolving threats effectively. Scalable AI systems allow the institutions to identify, respond to and prevent fraud in real-time, reducing manual workloads and resulting in increased operational efficiency.

The institution must develop a quick-workable, long-term strategy to scale AI-driven fraud solutions by focusing on some key areas:

1. Use a mix of AI and existing rule-based systems. This helps ensure smooth transition, better comparisons, fewer work disruptions and full compliance with regulations.
2. Build real-time big data systems using cloud technology and advanced analytics. This allows quick processing of millions of transactions and faster fraud detection.

3. Keep updating and training AI models with new data. This helps them stay alert to new fraud tricks and maintain high accuracy.
4. Focus on transparency and control. Use explainable AI tools so everyone including staff, regulators and partners can understand how decisions are made. Support this with strong governance and compliance systems.
5. Work closely with external partners and vendors to share fraud intelligence across the industry. This helps identify and stop new fraud patterns early.
6. Automate document checks and compliance work. This saves time and handles heavy workloads efficiently, especially during busy periods.
7. Use machine learning to create dynamic risk scoring systems. These continuously assess transactions and behaviors, allowing flexible fraud detection without adding extra pressure on teams.

MS: The Economic Survey flagged that while AI can revolutionise banking, risks like black-box systems, human oversight loss and cybersecurity threats remain significant. What governance architecture should India's financial institutions establish to make sure AI-driven decision-making remains explainable, auditable and aligned with regulatory norms?

Mr. Saad: To make sure AI-based decisions in finance can be checked, trusted and meet all rules, banks and financial institutions need a strong system of governance and assurance. This means having clear policies, defined responsibilities and regular monitoring; all in line with ethical and legal standards.

The Reserve Bank of India released the **FREE-AI Framework (Framework for Responsible and Ethical Enablement of Artificial Intelligence) in August 2025.** It emphasises on several key principles such as trust, fairness, accountability and explainability; that all financial institutions must follow. This ensures that AI decisions are explainable, auditable and reviewed at the board level under clear AI policies.

A good AI governance system should match the organisation's values and policies. It should include risk assessment, ethical review and close supervision so that all AI decisions can be traced and audited. Each team, from data scientists to compliance officers, must have clear roles defined. Recording every step of the AI process, including data, algorithms and reasoning, builds public trust. Tools like audit trails and explainability layers help make the process transparent.

Continuous automated monitoring is also needed to check performance, bias and compliance and to raise real-time alerts when needed. **Following global standards like ISO 42001 and the NIST AI Risk Management Framework supports global alignment.** For major decisions, human review should remain in place to ensure ethical judgment. Regular staff training and policy updates help the system stay current with new regulations.

With this transparent, multi-disciplinary approach, financial institutions can achieve responsible and auditable AI innovation, maintaining both trust and compliance while advancing technology.

MS: A survey found 82% of enterprises in India use data analytics only moderately or not at all in audit functions; only 18% use it extensively. How should India's financial institutions and regulators elevate the use of advanced analytics in internal and external audits to bolster governance?

Mr. Saad: To make audits smarter and strengthen the governance, organisations should use a clear analytics governance framework that matches their business goals and regulatory requirements. They should form an analytics governance board with senior management support to guide and monitor all projects. This board should make sure that every audit has clear goals and proper records of all actions.

Analytics can be built directly into audit processes. This helps automate control checks and decision-making, making audits faster and more accurate. AI and machine learning can continuously assess risks, detect unusual patterns and prevent fraud. This allows auditors to take timely action instead of reacting later.

Strong data governance is needed to maintain data quality, protect privacy and follow compliance rules at every stage of the audit. Auditors should be trained in data literacy, analytical thinking and using technology effectively to get the best results from these tools.

Real-time dashboards and automated reports make audits more transparent and improve communication with stakeholders. They also help in continuous monitoring. It is important to use analytics ethically to ensure fairness, transparency and privacy.

With this approach, audits shift from being occasional checks to ongoing, data-driven processes. This brings deeper insights, better risk management and stronger governance that meet both business and regulatory standards.

MS: What regulatory safeguards and audit mechanisms should India’s banks and regulators implement to manage the compliance risks from fintech and non-bank financial-services tie-ups?

Mr. Saad: To manage compliance risks in fintech and non-bank financial services, the organisations need a proactive and layered governance system. It should focus on proper checking (due diligence), clear sharing of responsibilities and regular monitoring.

A strong governance setup means checking fintech partners carefully and monitoring their regulatory compliance, internal controls, financial strength and operational risks. Smaller fintechs may not have mature systems, so they need extra scrutiny. Every contract should clearly mention who is responsible for compliance, data privacy, customer protection and following AML, KYC and sanctions rules.

Regular oversight through audits, performance checks and automated tools helps catch and fix issues early. This reduces both regulatory and operational risks. Data security must be tightened using encryption and access monitoring to prevent cyberattacks. It’s also important to check a partner’s financial stability and ability to handle operational shocks.

Organisations must keep pace with changing laws on digital payments, deposits and customer information. Joint plans with partners for incident response and emergency situations help avoid disruptions and protect customers.

MS: How can audit functions within Indian financial institutions evolve to cover cyber-resilience, third-party risk, vendor governance and supply-chain risks (not just traditional financial audit)?

Mr. Saad: Audit work in financial institutions has grown far beyond just checking accounts and balance sheets. Today, it deals with many new risks like cybersecurity, third-party vendors and supply-chain issues.

This change has come because of fast digital growth, stricter regulations and higher operational risks. **Modern audits now include cybersecurity checks** such as penetration testing, finding system weaknesses and testing how ready an organisation is to respond to a cyberattack.

As banks and financial firms depend more on outside vendors and fintech partners, **audits also cover vendor risk management.** This means checking whether vendors follow laws, keep data safe, have proper internal controls and are regularly monitored to prevent disruptions and legal problems.

Advanced tools and data analytics now help auditors find risks and fraud in real time. This is making sure contracts and partnerships follow the latest rules.

In India, the audit function has become a mix of finance, technology and risk management. This combined approach protects financial institutions from financial, operational, cyber and compliance risks that helps maintain stability and meet regulatory expectations in a fast-changing world.

MS: The survey of Indian CAEs found that while 69% believe AI & ML will shape the future of internal audit, many admit gaps in use cases. What changes in audit planning, talent, tools and regulatory oversight are needed in India to ensure internal audit keeps pace with rapidly evolving risk, compliance and technology landscapes?

Mr. Saad: Internal audit in India needs to grow with changing risks, rules and technology. For this, there must be major improvements in how audits are planned, how people are trained, what tools are used and how regulators monitor the process.

Auditors should follow a flexible, risk-based plan that matches new business and regulatory priorities. Institutes must focus on digital transformation, using real-time data analysis and regularly checking high-risk areas like cybersecurity, third-party risks and AI governance.

Training and upskilling auditors are very important in this fast-changing environment. They need stronger skills in data analytics, cybersecurity and new technologies. Clear and regular communication between auditors, management and the board helps build trust and improves audit quality and the organisation's resilience.

Regulators are also updating their policies and standards to **strengthen audit independence, quality checks and board involvement.** Following the standards of the Institute of Chartered Accountants of India (ICAI) and the Institute of Internal Auditors (IIA) remains essential.

About Mohammad Saad

Mohammad Saad is a seasoned professional with a running 22 years of experience in the Banking and Financial Services sector. He has worked with leading organisations such as Barclays, American Express and ABN AMRO Bank. He holds an LLB degree and a Master's qualification and is also a Certified ISO 27001 Lead Auditor. Saad has wide experience in Internal Audit, Control Assurance, Enterprise Risk and Operational Risk Management for large business functions.

About the Interviewer

Mahima Sharma is an Independent Journalist based in Delhi NCR. She has been in the field of TV, Print & Online Journalism since 2005 and previously an additional three years in allied media. In her span of work she has been associated with CNN-News18, ANI - Asian News International (A collaboration with Reuters), Voice of India, Hindustan Times and various other top media brands of their times. In recent times, she has diversified her work as a Digital Media Marketing Consultant & Content Strategist as well. Starting March 2021, she is also a pan-India

Entrepreneurship Education Mentor at Women Will - An Entrepreneurship Program by Google in Collaboration with SHEROES. Mahima can be reached at media@indiastat.com

Disclaimer: This interview is the personal opinion of the interviewed protagonist and not those of the organisation he/she works for. The facts and opinions appearing in the answers do not reflect the views of Indiastat or that of the interviewer. Indiastat does not hold any responsibility or liability for the same.