The Dialogue®
INFORM ENGAGE IDEATE

CoRE-AI™
Coalition for Responsible Evolution of AI

ANALYSIS

DECODING FREE-AI

Insights into RBI framework for trustworthy AI in banking and beyond

October, 2025

ANALYSIS

DECODING FREE-AI INSIGHTS INTO RBI FRAMEWORK FOR TRUSTWORTHY AI IN BANKING AND BEYOND

Authors: Soham Jagtap and Ranjeet Rane
Research Assistant: Devanshi Kumar

The Dialogue® is a public policy think tank with a vision to drive a progressive narrative in India's policy discourse. Founded in 2017, we believe in facilitating well-researched policy debates at various levels to help develop a more informed citizenry, on areas around technology and development issues. The Dialogue® has been ranked as the world's Top 10 think tanks to watch out for, by the Think Tank and Civil Societies Programme (TTCSP), University of Pennsylvania in their 2020 and 2021 rankings.

For more information
www.thedialogue.co

Suggested Citation
Jagtap, S. & Rane, R. (October, 2025) Analysis: Decoding FREE-AI: Insights into RBI Framework for Trustworthy AI in Banking and Beyond. The Dialogue®

Catalogue No
TD/DE/ER/1025/08

Publication Date
October 1, 2025

Table of Contents

At a Glance

RBI's FREE-AI Report: Revolutionary Framework for Financial AI

India's financial sector is entering a new era with the Reserve Bank of India's groundbreaking FREE-AI Report - the country's first comprehensive regulatory framework for Artificial Intelligence in finance, released in August 2025.

26 Recommendations
Comprehensive guidelines across six critical pillars of AI implementation

Seven Sutras Foundation
Anchored in responsible AI principles for ethical financial services

Global Benchmarking
Aligned with EU AI Act, Singapore MAS, and international best practices

The Six Pillars Framework

Infrastructure
Building robust technological foundations for AI deployment in financial services

Governance
Board-level oversight and accountability for AI systems

Policy
Establishing clear regulatory guidelines and compliance frameworks

Protection
Safeguarding consumer rights and data privacy

Capacity
Developing talent and skills for responsible AI implementation

Assurance
Continuous monitoring and validation of AI systems

Key Implementation Areas & Strategic Impact

AI Governance Excellence

- Board-approved AI policies with clear accountability
- End-to-end model lifecycle management
- Comprehensive risk appetite frameworks
- Detailed AI model inventories and audit systems

Data Security & Protection

- Robust data lifecycle governance protocols
- Advanced cybersecurity for AI-specific threats
- Red-teaming and adversarial testing requirements
- Incident reporting and business continuity plans

Consumer-Centric Approach

- Transparent AI disclosures and explanations
- Accessible grievance mechanisms
- Ongoing consumer education programs
- Ethical AI decision-making processes

Global Alignment & Future Vision

EU AI Act
Comprehensive risk-based approach to AI regulation

Singapore MAS
FEAT and Veritas frameworks for responsible AI

IndiaAI Mission
National AI strategy and DPDP Act compliance

What's Next for Financial Institutions: The transition from recommendations to operational reality requires treating AI governance as a board-level priority, investing in talent and training, and preparing for expanded compliance including audits, disclosures, and red-teaming protocols.

1. Introduction

Announced in December 2024 by RBI, the Framework for Responsible and Ethical Enablement of Artificial Intelligence (FREE AI) committee was constituted to balance innovation with consumer risk management in AI adoption across financial services. The exponential application of AI in credit scoring, fraud detection, trading, and customer engagement led to rising concerns of bias, systemic risks and consumer protection which propelled the aforementioned. Through the committee's recommendations, the RBI hopes to nurture a hub of innovation complemented by adequate safeguards.

The committee undertook multiple surveys of regulated entities, consultations with banks, NBFCs, fintechs, and comparative review of international practices between January to July 2025. The FREE-AI report was released in August 2005, introducing the seven sutras as guiding principles and 26 recommendations under six pillars of Infrastructure, Policy, Capacity, Governance, Protection, and Assurance.

The Committee conducted two surveys that covered Scheduled Commercial Banks (SCBs), Non-Banking Financial Companies (NBFCs), Fintechs, and All India Financial Institutions (AIFIs) to understand AI adoption in financial services and associated challenges. The methodology further included stakeholder engagement, literature review and analysis of extant regulatory guidelines. The report provides actionable recommendations under an innovation enablement framework to remove barriers and accelerate AI adoption in the financial sector, and a risk mitigating framework to ensure safety and responsibility in AI deployment.

Under the innovation enablement framework, the three pillars include the infrastructure pillar, policy pillar and capacity pillar. Under the risk mitigation framework, the three pillars include the assurance pillar that recommended the creation of an AI audit framework for REs and an AI toolkit developed by a financial sector SRO to help REs validate adherence to key responsible AI principles; the protection pillar that recommends creation of a risk intelligence framework for AI incident reporting in the financial sector; and the governance pillar, that recommends a data lifecycle governance framework and an AI systems governance framework for REs.

This paper aims to present a comparative analysis of the FREE-AI recommendations against the global landscape of AI regulation in financial services. This was by analysing various regulatory approaches adopted across jurisdictions such as Singapore, UK, Brazil and Europe along with a report released by the Bank of International Settlements (BIS) on regulating AI in the financial services. Two key jurisdictions, namely the US and China have not been included in this analysis owing to the high policy uncertainty in the former and the lack of policy transparency of the latter.

The next section the recommendations made globally with what is recommended by the RBI, while examining alignment with the IndiaAI mission.

The final section shall frame strategic takeaways for banks and fintechs — what it means for their operations and strategic priorities.

2. Global Landscape Analysis

AI has been used in financial services for many years, with use cases such as chatbots, fraud detection, anti-money laundering and combating terrorist financing mechanisms (AML/CFT). The difference now is that these applications are much more advanced due to the exponential advancements in AI. Such advancements have brought transformative benefits, but consequently, have also exacerbated risks associated with the use of these technologies. In response to these, international and national authorities have introduced various AI-specific guidance for financial institutions.

Jurisdictions such as Singapore, the UK, Brazil, and the European Union have introduced frameworks that emphasise responsible AI principles, sector-specific guidelines, and supervisory toolkits. At the same time, international standard-setting bodies like the Bank for International Settlements (BIS) are working to harmonise regulatory thinking across borders. This section examines these developments, highlighting how different regulatory philosophies converge or diverge in addressing the unique risks and opportunities of AI in financial services.

2.1 Bank of International Settlements (BIS)

In December 2024, the Financial Stability Institute (FSI) of the BSI released a report titled *"Regulating AI in the financial sector: recent developments and main challenges".*[1] This report highlighted that various known risks in financial services are amplified with AI integration: credit risk, model risk, data privacy, cyber risk, operational risks, conduct risk, reputational risk, and systemic risk. The introduction of GenAI in particular, could lead to additional vulnerabilities such as concentration of third-party service providers, opacity, explainability challenges and cyber threats.

The BIS report highlights certain implementational issues including explainability, fair treatment, data governance and risk control issues in the use of AI in provision of core services such as credit and insurance. Further, the use of third-party AI models by major technology firms has raised questions pertaining to data security, operational resilience and accountability.

Interestingly, the report has noted that many jurisdictions have already got cross-sectoral AI guidance in place, hence the absence of sector-specific guidance, like in finance, can be argued. This is juxtaposed with the idea that industry players may be wary of investing in and bringing to the market transformative AI-based financial technology in the fear of future regulation. The report goes on to acknowledge that AI presents unique challenges in implementing existing financial regulations, positing the need for supervisory, sector-specific guidance. It highlights the need to examine existing regulations and consider issuing clarifications and guidance, particularly with reference to applications that are considered high risk and ought to have a significant impact on customers. For core services like credit and insurance underwriting, the report suggests that the entity must have a governance framework that makes the Board and senior management entirely accountable for all AI use cases. Further, it must clearly define roles and responsibilities across the entire AI lifecycle and whilst also including provisions to ensure human-in-the-loop (HITL) mechanisms. Next, the report recommends AI skilling of financial institutions' employees and management to effectively address AI-based risks. The report further recommends the need for model risk management to be put in place by financial institutions so as to curb risks part of AI use, such as lack of explainability.

For data governance and management, the report suggests that financial institutions' data governance and management tools must be evaluated in case of AI adoption, regardless of the fact that many aspects of the same are captured in existing regulations. There must be a method to gauge whether existing practices are sufficient to tackle increased vulnerabilities introduced by AI. For non-traditional

[1]Crisanto, J. C., Leuterio, C. B., Prenio, J., & Yong, J. (2024, December 12). *Regulating AI in the financial sector: Recent developments and main challenges* (FSI Insights on Policy Implementation No. 63). Bank for International Settlements. https://www.bis.org/fsi/publ/insights63.pdf

players and novel business models, the effectiveness of existing regulations must be gauged to identify gaps in current arrangements in the light of cross-sectoral use of AI.

Lastly, the report suggests a direct oversight mechanism for cloud service providers considering their concentration within a few global technology firms, observing that while some jurisdictions have opted for this method, many have doubled down on financial institutions' responsibility to be liable for the actions of the third parties.

In another report titled "*Governance of AI adoption in central banks*"[2], the BIS provided particular recommendations regarding how banks can identify, analyse, report and manage risks associated with the adoption of AI tools. The BIS sets the tone for a comprehensive risk management model that stresses on continuity with pre-existing financial frameworks to manage risks instead of building AI-specific legal regimes. This includes defining an AI risk appetite and setting clear boundaries on the level of acceptability, starting with low-risk internal processes before scaling it into critical operations and using a multidisciplinary evaluation process for AI projects. It also advocates for applying the "three lines of defence" model wherein as the first line of defence, operations & business units identify risks, set up monitoring mechanisms, deliver specialised training and implement controls. The second line of defence ensures AI use aligns with the central bank's risk appetite and profile. It develops risk methodologies, coordinates assessments, prioritises risks, updates policies for AI-specific risks, oversees compliance, provides training, and conducts technical and ethical audits.

The third line of defence provides independent, continuous reviews and recommendations to strengthen AI controls and policies, ensuring they adapt to evolving technologies and emerging risks.

What stands out in the report is the recommendation to adapt pre-existing international standards such as the ISO 27001, the NIST Cybersecurity Framework, and ISO/IEC 23894. Data protection throughout the AI life cycle, system explainability, third party and human oversight as well as validation are prioritised. Dedicated General Artificial Intelligence (GAI) policies are to be designed so as to address the occurrence of bias and ensure robustness and transparency, with warnings against shadow AI, i.e. unauthorised usage.

2.2 MAS (Monetary Authority of Singapore)

The MAS published an information paper titled "Artificial Intelligence Model Risk Management"[3] in December, 2024. This paper provides a comprehensive overview of best practices and observations from a thematic review on AI Model Risk Management (MRM) in banks, with a detailed emphasis on governance, identification, development, deployment, monitoring, and risk controls for AI, including Generative AI.

It recommends operationalising principles of fairness, ethics, accountability, and transparency (FEAT) to be through board-level accountability, cross-functional AI oversight forums, and dedicated AI committees. Firms are expected to maintain comprehensive AI inventories, document data lineage, purpose, inputs/outputs, classify risks by materiality, and subject these systems to independent validations, challenger models, and adversarial testing. They are also to update their risk policies to include AI, build staff capabilities, keep monitoring deployed AI, report incidents and keep humans in the loop. Further, the paper recommends independent validation or peer reviews tailored to AI risk levels, and establishing continuous post-deployment monitoring with clear thresholds.

Particularly for GenAI applications, the paper recommends limiting early GenAI use to assistive and internal purposes, apply human-in-the-loop oversight, establish detailed testing and evaluation, implement input/output guardrails, and ensure data security through private or controlled environments. In cases wherein internal AI controls are extended to third parties, best practices dictate

[2] Bank for International Settlements, Consultative Group on Risk Management. (2025, January 29). *Governance of AI adoption in central banks* (BIS Other Paper No. 90). https://www.bis.org/publ/othp90.pdf
[3] Monetary Authority of Singapore. (2024, December). *Artificial intelligence model risk management: Observations from a thematic review* [Information paper]. https://www.mas.gov.sg/-/media/mas-media-library/publications/monographs-or-information-paper/imd/2024/information-paper-on-ai-risk-management-final.pdf

conducting compensatory testing, adapting contracts with providers for transparency and performance guarantees, developing contingency plans, and enhancing training and awareness for staff.

The emphasis is not only on technical robustness but also on fairness, explainability, accountability, especially in retail settings where customer trust is fragile. This includes bias monitoring, transparency obligations to customers, and explicit prohibitions on unsafe generative AI usage (e.g., uncalibrated deployment in critical processes, self-modifying models, using sensitive data for training). Importantly, MAS uses its new "information papers" to set firm, non-negotiable standards, effectively turning recommended "good practices" into expected "supervisory requirements." Evidence requirements during inspections such as board minutes, shadow ai detection, etc. are other parts that showcase Singapore's proactive framework.

2.3 The European Union

The EU has provided member states with the overall framework and regulatory guidance through a sector-agnostic, technologically neutral legislation, the EU AI Act.[4] The EU AI Act inculcates AI oversight into a binding law with a tiered risk classification. Unacceptable risk applications such as social scoring and manipulative AI are outrightly banned. High-risk systems including those applied in the finance domain, face stringent regulatory requirements including technical documentation, transparency, cybersecurity, and registration in an EU-wide database.

Sector-specific regulators, such as the European Securities and Markets Authority (ESMA), have provided guidance to retail investment service providers on the use of AI. ESMA's approach emphasises a balance between fostering innovation through the adoption of AI and ensuring rigorous compliance with MiFID II[5], prioritising clients' best interests and robust risk management at all times. Its philosophy calls for transparency, strong governance, and continuous oversight to responsibly harness AI in retail investment services.[6] Similarly, European Insurance and Occupational Pensions Authority (EIOPA) has published guidance emphasising that while AI offers transformative potential across the insurance value chain, its deployment must ensure robust data governance, non-discrimination, and transparency, especially for high-risk systems under the new AI Act. EIOPA's approach underscores that AI innovation must proceed within the framework of existing insurance regulation, with enhanced governance, risk management, and consumer protection measures in line with the sector's responsibilities.[7]

Through the General Code of Practice of General Purpose Artificial Intelligence (GPAI), the EU AI Act encourages voluntary assurance to the Act's provisions pertaining to GPAI. Voluntary adherence gives an entity conditional immunity from administrative burden and additional legal certainty.[8] A study carried out by the European Banking Authority (EBA) highlighted that 40% of banks in the EU are already employing GPAI, although, majorly for customer support and optimisation of internal processes. The study deduces that EU banks have been adopting a risk-based approach to GPAI by building out guardrails, controls and ensuring human intervention during the early adoption of GPAI.[9]

[4]European Union. (2024, June 13). *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024*. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689

[5] https://eur-lex.europa.eu/eli/dir/2014/65/oj/eng

[6]European Securities and Markets Authority. (2024, May 30). *Public statement on the use of artificial intelligence (AI) in the provision of retail investment services* (ESMA35-335435667-5924). https://www.esma.europa.eu/sites/default/files/2024-05/ESMA35-335435667-5924__Public_Statement_on_AI_and_investment_services.pdf

[7]European Insurance and Occupational Pensions Authority. (n.d.). *Regulatory framework applicable to AI systems in the insurance sector* [Factsheet]. https://www.eiopa.europa.eu/document/download/b53a3b92-08cc-4079-a4f7-606cf309a34a_en?filename=Factsheet-on-the-regulatory-framework-applicable-to-AI-systems-in-the-insurance-sector-july-2024.pdf

[8]European Banking Authority. (2025). *Special topic – Artificial intelligence*. European Union. https://www.eba.europa.eu/publications-and-media/publications/special-topic-artificial-intelligence#ipn-0-5444760227677956

[9]European Banking Authority. (2025). *Special topic – Artificial intelligence*. European Union. https://www.eba.europa.eu/publications-and-media/publications/special-topic-artificial-intelligence#ipn-0-5444760227677956

2.4 Financial Conduct Authority

The FCA has adopted a principles-based, technology-agnostic, and outcomes-focused approach to regulating AI in financial services. Unlike prescriptive frameworks, its stance emphasises proportionality, flexibility, and consumer protection within existing regulatory structures. The FCA recognises that while many AI-related risks – such as data governance, operational resilience, and consumer harm – are not unique to AI, their scale and complexity require closer supervisory scrutiny.

It maps the UK Government's five AI principles to existing rules, stressing safety, fairness, transparency, accountability, and contestability. The FCA maps these principles against its existing regimes. For example, rules under the *Senior Management Arrangements, Systems and Controls* (SYSC) and the Senior Managers & Certification Regime (SM&CR) embed accountability and governance across the AI lifecycle, ensuring boards and senior management remain responsible for AI deployment. Consumer protection is reinforced through the *Consumer Duty*[10], which obliges firms to deliver fair outcomes, avoid foreseeable harm, and account for vulnerable consumers, which are critical safeguards when AI systems risk embedding bias or limiting access to services.

Operational resilience and third-party risks form another priority area. The FCA acknowledges that systemic reliance on a handful of AI or cloud service providers could create vulnerabilities, and it is exploring a framework for "Critical Third Parties" (CTPs) that could extend to systemic AI providers. In parallel, the FCA has highlighted competition risks arising from big tech dominance in AI models and cloud infrastructure, working closely with the Competition and Markets Authority to monitor data asymmetries and potential market distortions.[11]

Transparency and explainability obligations apply to firms' communications and automated decisions, supported by UK GDPR safeguards. The FCA itself uses AI for market surveillance, scam detection, and synthetic data testing. Looking ahead, it plans to expand empirical research with the Bank of England (BoE), test AI through its Digital Sandbox and Regulatory Sandbox, and explore a dedicated Artificial Intelligence (AI) Sandbox, while engaging internationally through the International Organization of Securities Commissions (IOSCO), the Financial Stability Board (FSB), the Organisation for Economic Co-operation and Development (OECD), and the G7.[12]

2.5 Banco Central do Brasil (BCB)

Brazil's Central Bank epitomises a marked innovation-driven strategy. It embeds AI into its broader national AI strategy[13] and embodies the principle through sandboxes, SupTech tools, and integration with its flagship payment system, Pix. AI is primarily used for fraud detection, credit monitoring, and resilience of payment rails through multiple circulars. Unlike the EU's expansive legal framework or MAS's governance-heavy regime, Brazil opts for rapid testing, sector-specific interventions, and gradual supervision.

The approach has both opportunities and limitations. On one hand where BCB's alignment of AI with national innovation makes it a driver of financial modernization, a lack of comprehensive AI-specific legal obligations leaves firms with vagueness, especially if risks translate beyond payments. In a crux, in Brazil compliance means aligning with Pix-centric rules, prioritizing fraud controls, and treating sandboxes as the sole drivers to growth. Recently, BCB reinforced this stance through the creation of a Center of Excellence for Data Science and Artificial Intelligence (CDE IA)[14], a consultative body tasked

[10]Financial Conduct Authority. (2022, July 27). *PS22/9: A new Consumer Duty — Feedback to CP21/36 and final rules*. https://www.fca.org.uk/publications/policy-statements/ps22-9-new-consumer-duty
[11]Financial Conduct Authority. (2024, April 22). *Potential competition impacts from the data asymmetry between Big Tech firms and firms in financial services* (Feedback Statement FS24/1). https://www.fca.org.uk/publication/feedback/fs24-1.pdf
[12]Financial Conduct Authority. (2024, April). *AI update*. https://www.fca.org.uk/publication/corporate/ai-update.pdf
[13]OECD. (2025). *Brazilian strategy for artificial intelligence*. OECD. https://www.oecd.org/en/publications/access-to-public-research-data-toolkit_a12e8998-en/brazilian-strategy-for-artificial-intelligence_936c5793-en.html
[14]Hall, I. (2024, August 23). Brazil's central bank creates "centre of excellence" for data science and AI. *Global Government Fintech*. https://www.globalgovernmentfintech.com/banco-central-do-brasil-centre-of-excellence-data-science-ai/

with setting governance guidelines for AI adoption and establishing requirements for generative AI systems. This institutionalises AI oversight within the Central Bank, though still with an emphasis on flexible and innovation-friendly governance rather than binding sectoral regulation.

3. Analysis of FREE-AI report's key recommendations

In this section, the FREE-AI report's key recommendations, starting from Chapter 4 of the report, which are directed to the Regulated Entities (REs), Self-Regulatory Organisations (SROs) and the industry have been analysed, contrasted with best practices followed in other jurisdictions and then weighed up against the goals of the IndiaAI mission.

3.1 Capacity Building within REs

REs should develop AI- related capacity and governance competencies for the Board and C suite, as well as structured and continuous training, upskilling, and reskilling programs across the broader workforce who use AI, to effectively mitigate AI risks and guide ethical as well as ensure responsible AI adoption.

This recommendation is given under the capacity pillar. It is suggested that decision makers as well as the broader workforce within the RE must be equipped with the necessary skills and training to ensure responsible adoption and usage of AI applications. The report recommends hiring board members with specific AI governance expertise and distinguishing AI expertise from general IT expertise.

The report further recommends collaboration between financial institutions, training providers, Edtech and academia. It also recommends institutes of excellence such as IITs and IIMs to provide tailored courses on AI in finance. The report pushes for the development of scalable and inclusive capacity building programs that can reach the wider workspace spanning in smaller institutions and rural branches.

Through the *Master Direction on Outsourcing of Information Technology Services,* the RBI had mandated the Senior Management of REs to create capacity within the organisation to carry out oversight of outsourced activities.[15] A similar regulatory mandate can be created by the RBI and other sectoral regulators to ensure that REs have AI competencies in place across the board. This could tie in with Recommendation 6 of the report that urges regulators to formulate comprehensive AI policy frameworks for the financial sector.

Alignment with the IndiaAI Mission: The recommendation directly references the IndiaAI mission, particularly the AI Competency Framework[16] developed by MeitY, suggesting REs to take reference from the same to develop their capacity building initiatives. This recommendation aligns with the IndiaAI mission, given its focus on AI talent and workforce development that can be illustrated by various efforts under the IndiaAI mission to make India a global destination for R&D and technological development.

Global Comparison: The FCA emphasizes sector-specific AI governance through a principles-based approach, requiring financial institutions to demonstrate board-level AI expertise distinct from general IT competencies.[17] The regulator actively promotes capacity building through its AI and Digital Hub,

[15]Reserve Bank of India. (n.d.). *Clause 11(g) [Review of Clause 11(g)].* https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?Id=12486

[16]India. Ministry of Electronics and Information Technology. (2024, December). *Empowering public sector leadership: A competency framework for AI integration in India* (Report). https://indiaai.s3.ap-south-1.amazonaws.com/docs/empowering-public-sector-leadership.pdf

[17]Financial Conduct Authority. (n.d.). *AI approach*. https://www.fca.org.uk/firms/innovation/ai-approach

providing targeted guidance on responsible AI adoption, risk mitigation frameworks, and specialized training initiatives.[18]

The EU's AI Act imposes the most prescriptive capacity building requirements globally for financial services, mandating that high-risk AI systems used in financial applications require specialized governance competencies at board and senior management levels[19]. Financial institutions must provide structured training on ethical AI use and specific AI Act requirements to all relevant staff, distinguishing between AI proficiency and traditional IT skills. The Act requires comprehensive workforce upskilling programs, documented AI literacy initiatives, and regular competency assessments. Enforcement responsibility falls to financial supervisory authorities including the EBA, ESMA, and EIOPA, who are expected to evaluate institutions' AI governance frameworks and capacity building programs as part of their supervisory activities.[20,21]

Singapore's MAS has developed the most comprehensive collaborative capacity building framework through its Pathfinder Programme (PathFin.ai)[22], which brings together over 30 financial institutions to share AI implementation experiences and best practices.[23] MAS requires financial institutions to establish dedicated AI functions with specialized governance expertise, with several serving as Global AI Competency Centers. The regulator is developing an AI Governance Handbook in collaboration with the MindForge consortium and emphasizes structured workforce transformation through partnerships with training providers.[24] MAS's approach includes piloting generative AI applications across multiple job roles to understand workforce transformation needs and inform sector-wide training strategies.

3.2 Framework for Sharing Best Practices

The financial services industry, through bodies such as IBA or SROs, should establish a framework for the exchange of AI-related use cases, lessons learned, and best practices and promote responsible scaling by highlighting positive outcomes, challenges, and sound governance frameworks.

Information sharing is an important aspect that must be operationalised within the financial sector, especially when AI is adopted across various applications. Hence, this recommendation calls for a structured framework for financial institutions to share experiences, lessons and best practices. A voluntarily agreed upon framework shall assist industry players in determining their best courses of action during times of crisis and otherwise too.

Information sharing practices are considered an effective strategy to combat fraud, especially in the context of fast payments. Financial institutions benefit from clear rules around information sharing and disclosure.[25] Replication of this strategy in instances of AI adoption is expected to have the same effect. AI is an emerging technology, and the benefits and pitfalls of its various applications, especially in the financial sector, are yet to be gauged fully. An information sharing framework is expected to bridge this gap, and give financial institutions the confidence and security to adopt AI in their operations.

[18]Financial Conduct Authority. (n.d.). *AI approach*. https://www.fca.org.uk/firms/innovation/ai-approach
[19]European Union. (2024, June 13). *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024*. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689
[20]European Securities and Markets Authority. (2024, May 30). *ESMA provides guidance to firms using artificial intelligence in investment services* (Public Statement ESMA35-335435667-5924). https://www.esma.europa.eu/press-news/esma-news/esma-provides-guidance-firms-using-artificial-intelligence-investment-services
[21]European Insurance and Occupational Pensions Authority. (2024, July 15). *Factsheet on the regulatory framework applicable to AI systems in the insurance sector* [Factsheet]. https://www.eiopa.europa.eu/publications/factsheet-regulatory-framework-applicable-ai-systems-insurance-sector_en
[22]**Monetary Authority of Singapore.** (n.d.). *PathFin.ai: MAS pathfinder programme*. https://www.mas.gov.sg/schemes-and-initiatives/pathfinai
[23]IBS Intelligence. (2025, July 16). *MAS Pathfinder to help financial firms adopt AI responsibly*. https://ibsintelligence.com/ibsi-news/mas-pathfinder-to-help-financial-firms-adopt-ai-responsibly/
[24]**Monetary Authority of Singapore.** (2024, May 27). *Project MindForge*. https://www.mas.gov.sg/schemes-and-initiatives/project-mindforge
[25]LexisNexis Risk Solutions. (n.d.). *Collaboration can help fight fraud*. https://risk.lexisnexis.com/global/en/insights-resources/article/collaboration-can-help-fight-fraud

Alignment with the IndiaAI Mission: Although the IndiaAI mission does not directly address information sharing among industries to ease AI adoption, it does so indirectly by advocating for democratised access to AI, conceptualised through affordable compute power, data centres and AI-enabled DPI.

Global Comparison: The UK's FCA has established comprehensive information sharing mechanisms through its AI Lab initiatives, including the AI Spotlight program that enables financial institutions to share real-world insights on AI implementation across key themes such as bias, fairness, explainability, and governance.[26] The FCA's AI Sprint brings together industry professionals, academics, regulators, and consumer representatives to facilitate knowledge exchange and inform regulatory approaches.[27] Through its collaborative frameworks with the Global Financial Innovation Network, the FCA promotes cross-border sharing of AI best practices and regulatory experiences, emphasizing the importance of international cooperation in developing consistent AI governance standards.[28,29]

The EU's approach to information sharing is embedded within the AI Act's governance structure, requiring financial institutions to cooperate with supervisory authorities and share AI-related information for compliance assessment.[30] The Act establishes formal channels for information exchange between financial supervisors (EBA, ESMA, EIOPA) and mandates that deployers of high-risk AI systems cooperate with competent authorities in regulatory actions.[31] The EU framework also promotes industry collaboration through shared responsibility models for third-party AI systems, encouraging financial institutions to share experiences and best practices in managing AI-related risks and compliance requirements.[32]

Singapore's MAS has created the most structured collaborative framework through its PathFin.ai programme, which specifically brings together over 30 financial institutions to share AI implementation experiences and develop common best practices.[33] The regulator facilitates information sharing through Project MindForge[34], a collaboration between MAS and key banking, insurance, and capital market partners to develop frameworks for responsible generative AI use and solve industry-wide challenges.[35] MAS's approach emphasizes cross-functional AI oversight forums within institutions and sector-wide knowledge sharing through partnerships with training providers and academic institutions, creating a comprehensive ecosystem for AI best practice exchange.[36]

The BIS strongly advocates for central bank collaboration and knowledge sharing through its "community of practice" approach, emphasizing the pooling of resources, sharing of data and best

[26]Global Financial Innovation Network (GFIN), *et al.* (2025). *The GFIN AI report 2025: Key insights on the use of consumer-facing AI in global financial services*. https://www.thegfin.com/uploads/publications/pdf/1737980082_The%20GFIN%20Ai%20Report%202025.pdf
[27]Financial Conduct Authority. (2024). *AI update*. https://www.fca.org.uk/publication/corporate/ai-update.pdf
[28]Meakin, H., & Dulieu, R. (2025, July 2). *AI regulation in financial services: FCA developments and emerging enforcement risks*. Regulation Tomorrow. https://www.regulationtomorrow.com/eu/ai-regulation-in-financial-services-fca-developments-and-emerging-enforcement-risks/
[29]Henderson, A., Barwick, G., Scott, G., Taylor, J., & Dixon-Ward, M. (2024, April 25). *The FCA's AI Update: Integrating the UK Government's 5 Principles*. Goodwin Law. https://www.goodwinlaw.com/en/insights/publications/2024/04/alerts-finance-aiml-the-fca-ai-update
[30]Salloum, D. (2024, August 5). *What the EU AI Act means for financial institutions*. Eastnets. https://www.eastnets.com/blog/blog/what-the-eu-ai-act-means-for-financial-institutions
[31]Protiviti. (2025, January 7). *The EU AI Act: The impact on financial services institutions*. Consultancy.eu. https://www.consultancy.eu/news/11237/the-eu-ai-act-the-impact-on-financial-services-institutions
[32]Henderson, A., Scott, G., Moille, C., & Dixon-Ward, M. (2024, August 9). *EU AI Act: Key points for financial services businesses*. Goodwin Law. https://www.goodwinlaw.com/en/insights/publications/2024/08/alerts-practices-pif-key-points-for-financial-services-businesses
[33]TechNode Global Staff. (2025, July 16). *Singapore launches Pathfinder program to help financial institutions adopt AI*. TechNode Global. https://technode.global/2025/07/16/singapore-launches-pathfinder-program-to-help-financial-institutions-adopt-ai/
[34] https://www.mas.gov.sg/schemes-and-initiatives/project-mindforge
[35]Monetary Authority of Singapore. (2024, May 27). *Project MindForge*. https://www.mas.gov.sg/schemes-and-initiatives/project-mindforge
[36]Monetary Authority of Singapore. (2024, December). *Artificial intelligence model risk management: Observations from a thematic review* [Information paper]. https://www.mas.gov.sg/-/media/mas-media-library/publications/monographs-or-information-paper/imd/2024/information-paper-on-ai-risk-management-final.pdf

practices, and collaborative development of AI tools and trained models.[37] BIS guidelines recommend establishing dedicated repositories for sharing open source code and AI models within the central banking community, facilitating joint procurement of commercial data, and conducting collaborative workshops and conferences for staff training.[38] The BIS framework specifically addresses the benefits of cooperation in reducing costs, improving efficiency, and leveraging synergies while maintaining data confidentiality through shared models without direct data sharing.[39]

Brazil's approach combines regulatory coordination with collaborative industry engagement through its National AI Strategy and the Centre of Excellence in Data Science and AI within the Central Bank.[40] The framework promotes data sharing and reuse through government databases and encourages collaborative models between government, industry, academia, and civil society. Brazil's regulatory structure includes permanent collaboration forums (CRIA) and technical cooperation agreements with sectoral authorities, facilitating systematic information sharing and best practice exchange.[41] The Brazilian model also emphasizes public-private partnerships in developing AI governance frameworks and training programs, creating comprehensive platforms for industry-wide collaboration.

3.3 Board-Approved AI Policy

To ensure the safe and responsible adoption of AI within institutions, REs should establish a board-approved AI policy which covers key areas such as governance structure, accountability, risk appetite, operational safeguards, auditability, consumer protection measures, AI disclosures, model life cycle framework, and liability framework. Industry bodies should support smaller entities with an indicative policy template.

The Committee requires every RE to adopt a board-approved AI policy that squarely assigns accountability and sets the firm's risk appetite, governance structure, controls, auditability, disclosures, consumer-protection commitments, model-lifecycle requirements, and liability posture. This policy is also expected to classify AI use cases by risk and align the organization's approach to its values and applicable regulation. The report explains why a single, formal policy is needed: without it, teams improvise, risk interpretations diverge, blind spots grow, and boards can be left unaware of reputational and prudential exposure. It also encourages industry bodies/self-regulatory organisations to publish an indicative policy template that smaller REs can adapt, and even presents a suggested outline in the Annexure of the report..

Alignment with the IndiaAI Mission: A formal, board-approved policy operationalises multiple pillars of the IndiaAI Mission across safety, accountability, compute/data use, and inclusion. IndiaAI's programme aims to democratise compute and data, build indigenous capability, and ensure safe and trusted AI; a board-level policy is the necessary glue that binds those capabilities to day-to-day decision rights, guardrails, and disclosures inside REs.[42] As IndiaAI rolls out artefacts such as AI Kosh (datasets/models/toolkits) and Safe & Trusted AI solutions, REs will draw on them under a governance umbrella that the board explicitly owns. In short, IndiaAI provides public goods and rails; Recommendation 14 ensures each RE has the internal constitution to use them responsibly.

[37]Bank for International Settlements. (2025, June 29). *Annual Report 2024/25*. https://www.bis.org/about/areport/areport2025.pdf

[38]Bank for International Settlements, Consultative Group on Risk Management. (2025, January 29). *Governance of AI adoption in central banks* (BIS Other Paper No. 90). https://www.bis.org/publ/othp90.pdf

[39]Schubert, A., Harutyunyan, L., Hennings, K., Chitu, M., Peña, G., Lengelsen, L., Dubow, B., Vajanne, L., Pfister, C., McNeill, J., Monacelli, F., Osawa, N., Lee, J., Madani-Beyhurst, S., Toh, H. C., Binmayouf, I., Maravic, J., Douma, R., & Eken, A. A. (2015, January). *Data-sharing: Issues and good practices* (IFC Report No. 1). Bank for International Settlements. https://www.bis.org/ifc/events/7ifc-tf-report-datasharing.pdf

[40]Hall, I. (2024, August 23). Brazil's central bank creates 'centre of excellence' for data science and AI. *Global Government Fintech*. https://www.globalgovernmentfintech.com/banco-central-do-brasil-centre-of-excellence-data-science-ai/

[41]Zanatta, R. A. F., & Rielli, M. (2024, December 10). *The artificial intelligence legislation in Brazil: Technical analysis of the text to be voted on in the Federal Senate plenary*. Data Privacy Brasil. https://www.dataprivacybr.org/en/the-artificial-intelligence-legislation-in-brazil-technical-analysis-of-the-text-to-be-voted-on-in-the-federal-senate-plenary/

[42]Press Information Bureau. (2025, March 6). *India's AI revolution: A roadmap to Viksit Bharat*. Ministry of Electronics & Information Technology. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2108810

Global Comparison: Internationally, board-level accountability is becoming standard. In the EU, supervisory statements (e.g., ESMA) clarify that management bodies retain responsibility when using AI, including third-party models;[43] The EU AI Act reinforces governance and transparency expectations that firms must internalize via policies. In the UK, the FCA's work on synthetic data and governance likewise expects firms to embed AI into existing risk and control frameworks, not treat it as a side experiment.[44] Central-bank community guidance (BIS) similarly stresses three lines of defence and institutional control for AI.[45] RBI's push for a board-approved AI policy is therefore well-aligned with leading jurisdictions and arguably clearer in its sectoral focus.

3.4 Data Lifecycle Governance

REs must establish robust data governance frameworks, including internal controls and policies for data collection, access, usage, retention, and deletion for AI systems. These frameworks should ensure compliance with the applicable legislations, such as the DPDP Act, throughout the data life cycle.

REs must institute robust data-governance frameworks for AI, spanning collection, access, usage, retention, and deletion, with internal controls and policies that ensure compliance throughout the data lifecycle. The Committee explicitly references the Digital Personal Data Protection (DPDP) Act, 2023[46] and emphasises keeping sensitive customer/institutional data in secure, controlled environments, particularly when using open-source or external models. The goal is to prevent bias amplification and unreliable outcomes that flow from weak data controls and to build operational trust through concrete, auditable data practices.

Alignment with the IndiaAI Mission: IndiaAI's AI Kosh and broader data/computation pillars are intended to democratise access while upholding safety and trust. Recommendation 15 ties directly to those aims: by installing lifecycle controls at REs, firms can responsibly consume and contribute to high-quality datasets, use privacy-enhancing techniques, and respect consent/retention norms consistent with DPDP. The IndiaAI Mission's "Safe & Trusted AI" track and public commitments around data quality are best realised when REs implement lifecycle policies that make dataset provenance, transformations, and retention visible and governed.

Global Comparison: The UK's FCA requires financial institutions to establish comprehensive data accountability structures throughout AI lifecycles, emphasizing synthetic data governance, bias mitigation protocols, and auditable data pipelines that demonstrate clear lineage from collection through deletion.[47] The EU AI Act mandates the most prescriptive data lifecycle requirements globally, requiring high-risk AI systems to maintain representative, bias-checked datasets with detailed documentation integrating GDPR and DORA compliance, enforced through financial supervisory authorities evaluating data governance as core AI compliance.[48] Singapore's MAS implements detailed validation schema checks, metadata tagging systems, and data traceability requirements through its AI Model Risk Management framework, with specific controls for managing data drift and third-party data governance across AI supply chains.[49] The BIS emphasizes data management as foundational to AI governance, recommending central banks leverage existing metadata registries and statistical

[43]European Securities and Markets Authority. (2024, May 30). *Public Statement on AI and investment services* (ESMA35-335435667-5924). https://www.esma.europa.eu/sites/default/files/2024-05/ESMA35-335435667-5924_Public_Statement_on_AI_and_investment_services.pdf
[44]Financial Conduct Authority. (2025, August). *Generating and using synthetic data for models in financial services: Governance considerations*. https://www.fca.org.uk/publication/corporate/synthetic-data-models-financial-services-governance.pdf
[45]Bank for International Settlements. (2025, January 29). *Governance of AI adoption in central banks* (BIS Other Paper No. 90). https://www.bis.org/publ/othp90.pdf
[46]Ministry of Electronics and Information Technology. (2024, June). *The Digital Personal Data Protection Act, 2023* (No. 22 of 2023). https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf
[47]Financial Conduct Authority. (2025, August). *Generating and using synthetic data for models in financial services: Governance considerations*. https://www.fca.org.uk/publication/corporate/synthetic-data-models-financial-services-governance.pdf
[48]European Parliament & Council of the European Union. (2024, July 12). *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence* (OJ L 2024/1689). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689
[49]Monetary Authority of Singapore. (2024, December). *Artificial intelligence model risk management: Observations from a thematic review* [Information paper]. https://www.mas.gov.sg/-/media/mas-media-library/publications/monographs-or-information-paper/imd/2024/information-paper-on-ai-risk-management-final.pdf

standards while implementing AI-specific controls for confidentiality, integrity, and privacy throughout model lifecycles.[50] Brazil combines comprehensive algorithmic impact assessments with data governance evaluations, mandating data portability rights and interoperability standards while ensuring Lei Geral de Proteção de Dados (LGPD) compliance through its Central Bank's specific model governance guidelines for financial institutions.[51]

3.5 AI System Governance Framework

REs must implement robust model governance mechanisms covering the entire AI model lifecycle, including model design, development, deployment, and decommissioning. Model documentation, validation, and ongoing monitoring, including mechanisms to detect and address model drift and degradation, should be carried out to ensure safe usage. REs should also put in place strong governance before deploying autonomous AI systems that are capable of acting independently in financial decision-making. Given the higher potential for real-world consequences, this should include human oversight, especially for medium and high-risk use cases and applications.

REs must implement end-to-end model governance: design, development, validation, deployment, ongoing monitoring, and decommissioning. They're asked to document models, monitor performance and model drift/degradation, and integrate controls for explainability, fairness, and security. Critically, where autonomous AI is used for financial decision-making, REs must set strong governance and human oversight, with clear rules that specify tasks AI can perform autonomously and tasks requiring human intervention, especially in medium- and high-risk use cases. Liability remains with the RE—AI does not dilute accountability.

Alignment with the IndiaAI Mission: IndiaAI's investment in compute, datasets, and indigenous models needs a mirrored institutional operating system inside firms. Recommendation 16 supplies that by mandating repeatable, documented lifecycle practices and explicit human-in-the-loop thresholds—vital as REs adopt India-built models or fine-tune artefacts from AI Kosh. It complements the Mission's Safe & Trusted AI deliverables by ensuring that model assurance, drift detection, and incident handling are not ad hoc but embedded in day-to-day governance.

Global Comparison: The FCA mandates comprehensive AI lifecycle governance through existing frameworks, requiring robust testing, validation, and continuous monitoring with clear accountability for autonomous AI systems in financial decisions.[52] The EU AI Act imposes the most prescriptive requirements globally, mandating high-risk AI systems establish systematic risk management covering design through decommissioning, with detailed documentation, human oversight protocols, and integration with EBA/ESMA/EIOPA supervision.[53,54] Singapore's MAS requires cross-functional oversight forums, validation protocols throughout AI lifecycles, and specific controls for model drift and third-party AI systems, with detailed inventories and human oversight for autonomous applications.[55] The BIS framework proposes ten practical governance actions including interdisciplinary committees, comprehensive model inventories, continuous monitoring, and regular audits with incident reporting

[50]Bank for International Settlements. (2025, January 29). *Governance of AI adoption in central banks* (BIS Other Paper No. 90). https://www.bis.org/publ/othp90.htm

[51]Nemko Digital. (n.d.). *AI governance Brazil: Navigating policies & compliance*. https://digital.nemko.com/regulations/ai-governance-brazil

[52]Financial Conduct Authority. (2024, August). *AI Update*. https://www.fca.org.uk/publication/corporate/ai-update.pdf

[53]European Parliament & Council of the European Union. (2024, June 13). *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence* (OJ L 2024/1689). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689

[54]European Securities and Markets Authority. (2024, May 30). *Public Statement on AI and investment services* (ESMA35-335435667-5924). https://www.esma.europa.eu/sites/default/files/2024-05/ESMA35-335435667-5924_Public_Statement_on_AI_and_investment_services.pdfhttps://www.eiopa.europa.eu/document/download/b53a3b92-08cc-4079-a4f7-606cf309a34a_en?filename=Factsheet-on-the-regulatory-framework-applicable-to-AI-systems-in-the-insurance-sector-july-2024.pdf

[55]Monetary Authority of Singapore. (2024, December). *Artificial intelligence model risk management: Observations from a thematic review* [Information paper]. https://www.mas.gov.sg/-/media/mas-media-library/publications/monographs-or-information-paper/imd/2024/information-paper-on-ai-risk-management-final.pdf

throughout AI system lifecycles.[56] Brazil's Central Bank established a Centre of Excellence to develop lifecycle governance guidelines emphasizing validation protocols and enhanced human oversight for generative AI applications, combining regulatory coordination with practical implementation guidance.[57]

3.6 Product Approval Process

REs should ensure that all AI-enabled products and solutions are brought within the scope of the institutional product approval framework, and that AI-specific risk evaluations are included in the product approval frameworks.

All AI-enabled products and solutions must fall within the RE's product-approval framework, with AI-specific risk evaluations added across the lifecycle, from pre-development and testing to deployment and monitoring. Evaluations should cover fairness/bias, explainability, consumer protection, cybersecurity, compliance, data quality and preprocessing, output sampling/back-testing, expert review, and feedback loops. REs are encouraged to use internal AI sandboxes for controlled testing, and ensure independence between evaluators and the model-development teams.

Alignment with the IndiaAI Mission: IndiaAI is scaling public infrastructure such as compute resources, the AI Kosh, and Safe & Trusted solutions while fostering innovation in the AI ecosystem. Recommendation 17 ensures that responsible entities do not release innovations without structured approvals. It institutionalizes the practice of responsible release by requiring AI-specific checks before products are delivered to customers. This approach aligns with IndiaAI's emphasis on safety and inclusion and ensures that the public-sector push for AI enablement matches the private sector's rigor in product development. This alignment protects consumers and accelerates credible adoption of AI technologies.[58]

Global Comparison: The UK's FCA integrates AI-specific risk assessments into its existing product approval regime, requiring firms to conduct fairness, explainability, and cybersecurity evaluations before authorisation and to maintain independent challenge functions throughout the AI product lifecycle.[59] Pilot programmes through its AI and Digital Hub sandbox allow controlled testing under regulatory oversight, ensuring robust consumer protection and operational resilience.

Under the EU AI Act, all high-risk AI systems including financial products must undergo mandatory conformity assessments prior to market entry, covering data quality, bias mitigation, transparency, and human oversight provisions.[60] Notified bodies or internal compliance units certify adherence to strict technical documentation and post-market monitoring requirements, with supervision by EBA, ESMA, and EIOPA.

Singapore's MAS requires financial institutions to integrate AI risk reviews into their product governance frameworks, mandating pre-launch validation of model performance and back-testing under its AI

[56]Bank for International Settlements. (2025, January 29). *Governance of AI adoption in central banks* (BIS Other Paper No. 90). https://www.bis.org/publ/othp90.pdf
[57]Hall, I. (2024, August 23). Brazil's central bank creates 'centre of excellence' for data science and AI. *Global Government Fintech*. https://www.globalgovernmentfintech.com/banco-central-do-brasil-centre-of-excellence-data-science-ai/
[58]IndiaAI. (2024, March 12). *Cabinet approves India AI mission at an outlay of ₹10,372 crore*. https://indiaai.gov.in/news/cabinet-approves-india-ai-mission-at-an-outlay-of-rs-10-372-crore
[59]Financial Conduct Authority. (2024, April). *AI Update*. https://www.fca.org.uk/publication/corporate/ai-update.pdf
[60]European Parliament & Council of the European Union. (2024, June 13). *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828* (OJ L 2024/1689). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689

Model Risk Management guidelines.[61] MAS's PathFin.ai pilots offer sector-wide sandboxes and expert challenge panels to vet AI solutions, ensuring independent evaluation and structured feedback loops.[62]

The BIS recommends that central banks adopt formal AI product approval protocols mirroring those for novel financial instruments, with multidisciplinary review committees assessing model development, security, and governance controls. BIS guidance emphasises the use of internal proof-of-concept environments and periodic re-certification to manage evolving AI risks.[63]

Brazil's Central Bank has extended its Open Finance product approval process to include AI tools, requiring fairness audits, explainability reports, and independent expert reviews before granting approval. Its Centre of Excellence issues standardized evaluation templates and convenes cross-sector panels to adjudicate AI product readiness, balancing innovation with consumer safeguards.[64]

3.7 Consumer Protection

REs should establish a board-approved consumer protection framework that prioritises transparency, fairness, and accessible recourse mechanisms for customers. REs must invest in ongoing education campaigns to raise consumer awareness regarding safe AI usage and their rights.

REs should implement a board-approved consumer-protection framework for AI that prioritises transparency, fairness, and accessible redress. Customers should be told when and how AI is used, what rights they have, and how to seek remedy. The report calls for ongoing consumer education so people understand safe AI use and can spot risks. In essence: put people first, explain AI interactions clearly, design recourse that actually works, and measure outcomes for disparate impact.

Alignment with the IndiaAI Mission: IndiaAI's "Safe & Trusted AI" pillar (including the roll-out of responsible-AI tools on AI Kosh) underlines a societal commitment to trustworthy, inclusive AI. Recommendation 18 translates that societal aim into customer-facing commitments within each RE—clear notices, opt-outs/alternatives where appropriate, grievance routes, and education campaigns. As IndiaAI invests public funds and credibility in AI adoption, this ensures consumer trust keeps pace with innovation and that vulnerable users are not left behind.

Global Comparison: The UK's FCA requires firms to publish clear AI disclosure statements for customers, explaining when AI is used and how decisions are made.[65] Its Consumer Duty framework mandates fair outcomes monitoring and accessible redress channels, supported by public guidance and targeted financial education campaigns.[66]

The EU's Consumer Credit Directive[67] and Digital Services Act[68] introduce mandatory transparency requirements for AI in financial products, requiring institutions to inform consumers of automated decision-making and provide human intervention options. Regulators enforce fairness impact

[61]Monetary Authority of Singapore. (2024, December). *Artificial intelligence model risk management: Observations from a thematic review* [Information paper]. https://www.mas.gov.sg/-/media/mas-media-library/publications/monographs-or-information-paper/imd/2024/information-paper-on-ai-risk-management-final.pdf
[62]Monetary Authority of Singapore. (2025, August 1). *PathFin.ai: MAS Pathfinder programme*. https://www.mas.gov.sg/schemes-and-initiatives/pathfinai
[63]Bank for International Settlements. (2025, January 29). *Governance of AI adoption in central banks* (BIS Other Paper No. 90) https://www.bis.org/publ/othp90.pdf
[64]Hall, I. (2024, August 23). *Brazil's central bank creates "centre of excellence" for data science and AI*. Global Government Fintech. https://www.globalgovernmentfintech.com/banco-central-do-brasil-centre-of-excellence-data-science-ai/
[65]Financial Conduct Authority. (2024). *AI update*. https://www.fca.org.uk/publication/corporate/ai-update.pdf
[66]Financial Conduct Authority. (2022, July 27). *PS22/9: A new Consumer Duty — feedback to CP21/36 and final rules*. https://www.fca.org.uk/publications/policy-statements/ps22-9-new-consumer-duty
[67]European Parliament & Council of the European Union. (2023, October 18). *Directive (EU) 2023/2225 of the European Parliament and of the Council on credit agreements for consumers and repealing Directive 2008/48/EC*. Official Journal of the European Union. https://eur-lex.europa.eu/eli/dir/2023/2225/oj/eng
[68]European Commission. (n.d.). *Digital Services Act*. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en

assessments and require member states to establish consumer education programs on AI rights and risks.

Singapore's MAS integrates AI consumer protections into its Fairness, Ethics, Accountability and Transparency (FEAT) guidelines.[69] Financial institutions must provide plain-language AI disclosures, maintain dedicated grievance processes, and conduct regular customer surveys to measure understanding.[70] MAS sponsors nationwide workshops and digital literacy initiatives focused on AI and financial services.[71]

The BIS highlights consumer protection as a core principle in its AI governance guidance, recommending institutions implement transparent AI disclosures, accessible complaint mechanisms, and ongoing public outreach. BIS encourages central banks to collaborate with consumer groups and conduct periodic reviews of AI impacts on different demographic segments.[72]

Brazil's Central Bank has issued mandatory consumer-protection rules for AI applications in banking, requiring prominent AI usage notices, simplified appeals processes, and compulsory financial literacy modules on AI risks.[73] Its Open Finance framework includes standardized consumer rights statements and supports public awareness campaigns through partnerships with consumer associations.[74]

3.8 Cybersecurity Measures

REs must identify potential security risks on account of their use of AI and strengthen their cybersecurity ecosystems (hardware, software, processes) to address them. REs may also make use of AI tools to strengthen cybersecurity, including dynamic threat detection and response mechanisms.

REs must identify AI-specific security risks and strengthen cybersecurity across hardware, software, and processes. The FREE-AI Committee encourages AI-native defense like dynamic threat detection, anomaly spotting, and rapid-response tools to counter novel attack vectors such as data poisoning, adversarial inputs, prompt injection, and data exfiltration via model endpoints. Consumer education on AI-related cyber risks is key. AI introduces new risks but also enables mitigations, so defense-in-depth tailored to AI use is essential. This aligns with RBI's FREE-AI Framework, which emphasizes robust governance, incident reporting, and real-time monitoring.

Alignment with the IndiaAI Mission: IndiaAI explicitly treats cybersecurity as a public-good and capability challenge (e.g., CyberGuard hackathons; Safe & Trusted components), and calls for secure compute and responsible model use. Recommendation 19 gives REs an implementation path: integrate AI-aware threat modelling, monitoring, and response; test and red-team models; educate customers; and ensure alignment with DPDP and sectoral cyber norms. This marries IndiaAI's ecosystem investments with institution-level resilience.

Global Comparison: The UK's FCA integrates AI-specific cyber risk assessments into its existing cybersecurity requirements, expecting firms to identify novel threats such as adversarial attacks and

[69]Monetary Authority of Singapore. (2022, December 19). *Principles to promote fairness, ethics, accountability and transparency (FEAT) in the use of artificial intelligence and data analytics in Singapore's financial sector*. https://www.mas.gov.sg/~/media/MAS/News%20and%20Publications/Monographs%20and%20Information%20Papers/FEAT%20Principles%20Final.pdf

[70]Monetary Authority of Singapore. (2024, December). *Artificial intelligence model risk management: Observations from a thematic review* [Information paper].https://www.mas.gov.sg/-/media/mas-media-library/publications/monographs-or-information-paper/imd/2024/information-paper-on-ai-risk-management-final.pdf

[71]Monetary Authority of Singapore. (2023, May 22). *MAS strengthens collaboration between financial institutions and training institutes to enhance artificial intelligence and data analytics skills*. https://www.mas.gov.sg/news/media-releases/2023/mas-strengthens-collaboration-between-fis-and-training-institutes

[72]Bank for International Settlements. (2025, January 29). *Governance of AI adoption in central banks* (BIS Other Paper No. 90). https://www.bis.org/publ/othp90.pdf

[73]Mattos Filho. (2025, May 5). *Brazil's Central Bank presents regulatory priorities for 2025 and 2026*. https://www.mattosfilho.com.br/en/unico/bcb-regulatory-priorities-2025-2026/

[74]Central Bank of Brazil. (n.d.). *Open Finance*. https://www.bcb.gov.br/en/financialstability/open_finance

data poisoning.[75] It encourages the use of AI-driven security tools for dynamic threat detection and mandates regular red-team exercises under its Technology Resilience Principles.

The EU's Digital Operational Resilience Act (DORA) extends to AI systems by requiring financial institutions to perform threat intelligence sharing, conduct vulnerability scans on AI components, and implement incident response plans that address AI-specific vulnerabilities. Supervisors review AI risk reports as part of routine operational resilience assessments.[76]

Singapore's MAS includes AI cyber risk in its Technology Risk Management Guidelines, mandating proactive AI threat modelling, continuous monitoring of model endpoints for anomalies, and periodic penetration tests that simulate prompt injection and model inversion attacks. MAS supports public-private Cyber Week events to share AI-security best practices.[77]

The BIS guidance emphasises the need for defence-in-depth tailored to AI, recommending central banks adopt AI-native security measures such as automated anomaly detection and self-learning intrusion prevention. It promotes collaboration through shared cyber intelligence platforms among central banking communities.[78]

Brazil's Central Bank requires financial institutions to integrate AI risk into their cybersecurity frameworks, with mandatory testing of AI models for adversarial resilience and endpoint security. Its Centre of Excellence issues standardized playbooks for AI cyber-security and hosts multi-stakeholder drills to validate incident response capabilities.

3.9 Red Teaming

REs should establish structured red teaming processes that span the entire AI lifecycle. The frequency and intensity of red teaming should be proportionate to the assessed risk level and potential impact of the AI application, with higher risk models being subject to more frequent and comprehensive red teaming. Trigger-based red teaming should also be considered to address evolving threats and changes.

REs should institute structured, risk-proportionate red teaming across the full AI lifecycle, from model design and pre-deployment testing to post-deployment monitoring. "Higher-risk" models (e.g., those affecting credit decisions, fraud controls, or autonomous actions) should face more frequent and deeper exercises, while trigger-based red teaming kicks in after material changes (model retraining, new data sources, novel attack techniques) or observed drift. Red teaming should explicitly test for safety, security, bias, privacy leakage, prompt injection/jailbreaks, data poisoning, output manipulation, and distributional shift. The intent is to detect and close pathways to consumer harm and prudential risk before incidents occur and to generate actionable remediation tasks owned by accountable functions (risk, compliance, security, model risk). This embeds an adversarial mindset and evidence-based assurance into day-to-day operations.

Alignment with the IndiaAI Mission: IndiaAI's Safe & Trusted AI thrust and open artefacts (e.g., AI Kosh datasets/tools) are enablers, but Recommendation 20 is the operational safety layer inside firms. It creates a bridge between public-good infrastructure and enterprise-grade assurance, ensuring REs exercise adversarial testing before and after consuming IndiaAI resources. This dovetails with IndiaAI's emphasis on responsible adoption and governance capacity within institutions, not just access to data/compute.

[75]Financial Conduct Authority. (2024, April 22). *AI update: Further to the Government's response to the AI White Paper*. https://www.fca.org.uk/publication/corporate/ai-update.pdf
[76]European Insurance and Occupational Pensions Authority. (n.d.). *Digital Operational Resilience Act (DORA)*. https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en
[77]Monetary Authority of Singapore. (2021, January 18). *Technology Risk Management Guidelines*. https://www.mas.gov.sg/regulation/guidelines/technology-risk-management-guidelines
[78]Bank for International Settlements. (2025, January 29). *Governance of AI adoption in central banks* (BIS Other Paper No. 90) https://www.bis.org/publ/othp90.pdf

Global Comparison: The UK's FCA integrates AI red teaming into its existing cybersecurity framework, requiring financial firms to conduct adversarial testing as part of their Technology Resilience Principles. The FCA promotes structured red teaming through CBEST (Cyber Security Testing Framework) and has extended this to include AI-specific vulnerabilities such as prompt injection, data poisoning, and model inversion attacks.[79] Banks must demonstrate continuous testing capabilities and maintain independent challenge functions to validate AI system resilience.

The EU's Digital Operational Resilience Act (DORA)[80] mandates threat-led penetration testing for high-risk AI systems, requiring financial institutions to conduct regular red teaming exercises based on the TIBER-EU framework.[81] The Act specifically addresses AI-specific attack vectors and requires institutions to test for adversarial inputs, model manipulation, and bias exploitation. Financial supervisors evaluate red teaming programs as part of AI Act compliance assessments, with mandatory documentation of testing methodologies and remediation actions.

Singapore's MAS requires structured adversarial testing through its AI Model Risk Management framework, with specific guidance on red teaming generative AI systems.[82] The Association of Banks in Singapore has issued comprehensive guidelines mandating red teaming exercises during development, pre-deployment, and post-deployment phases, with particular focus on prompt injection, jailbreaking, and bias detection. Singapore has conducted the world's first multicultural AI safety red teaming challenge, establishing benchmarks for regional AI vulnerabilities.[83]

The BIS emphasizes red teaming as fundamental to AI governance in central banks, recommending systematic adversarial testing as part of its ten-action framework. BIS guidelines promote cross-border collaboration in red teaming exercises and advocate for shared testing methodologies among central banking communities. The framework emphasizes continuous monitoring, incident reporting, and regular reviews of red teaming effectiveness to address evolving AI threats.[84]

Brazil's Central Bank incorporates AI red teaming into its cybersecurity requirements through its Centre of Excellence in Data Science and AI, mandating regular adversarial testing of AI models used in financial applications. The framework requires institutions to test for prompt injection, data manipulation, and adversarial attacks, with specific attention to generative AI vulnerabilities.[85] Brazil's approach emphasizes collaborative red teaming exercises and knowledge sharing across financial institutions to address systemic AI risks

3.10 Business Continuity Plan for AI Systems

REs must augment their existing BCP frameworks to include both traditional system failures as well as AI model-specific performance degradation. REs should establish fallback mechanisms and periodically test the fallback workflows and AI model resilience through BCP drills.

REs must extend Business Continuity Planning (BCP) to AI-specific failure modes, not just traditional outages. Beyond infrastructure failover, BCP should cover model-performance degradation, data pipeline breaks, drift beyond thresholds, poisoned features, and third-party model/API unavailability. Firms should pre-define fallback mechanisms (rule-based or human-in-the-loop alternatives, feature-

[79]

[80]European Insurance and Occupational Pensions Authority. (n.d.). *Digital Operational Resilience Act (DORA)*. https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

[81]European Central Bank. (2018, May). *TIBER-EU Framework: How to implement the European framework for Threat Intelligence-based Ethical Red Teaming*. https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf

[82]Monetary Authority of Singapore. (2024, December 5). *Information paper on artificial intelligence model risk management* (ID 18/24). https://www.mas.gov.sg/-/media/mas-media-library/publications/monographs-or-information-paper/imd/2024/information-paper-on-ai-risk-management-final.pdf

[83]Association of Banks in Singapore. (2024, September). *Red team: Adversarial attack simulation exercise: Guidelines for the financial industry in Singapore*. https://www.abs.org.sg/docs/library/abs-red-team-adversarial-attack-simulation-exercises-guidelines----september-2024.pdf

[84]Bank for International Settlements. (2025, January 29). *Governance of AI adoption in central banks* (BIS Other Paper No. 90) https://www.bis.org/publ/othp90.pdf

[85]Hall, I. (2024, August 23). *Brazil's central bank creates 'centre of excellence' for data science and AI*. Global Government Fintech. https://www.globalgovernmentfintech.com/banco-central-do-brasil-centre-of-excellence-data-science-ai/

reduced models, throttling/kill-switches) and regularly drill those scenarios. The aim is continuity of critical services (payments, credit adjudication, fraud detection) when AI components misbehave or become unsafe, and fast, well-rehearsed recovery.

Alignment with the IndiaAI Mission: As IndiaAI expands safe data/compute access and promotes domestic AI capability, REs must be operationally ready for AI-specific resilience events. Recommendation 21 translates IndiaAI's safety aims into resilience playbooks inside firms, tying together risk, tech, and business owners. It also complements broader Indian regulatory objectives on operational resilience and consumer protection by ensuring graceful degradation and clear reversion paths when AI is impaired.

Global Comparison: The UK's FCA integrates AI into its established Business Continuity Planning under the Technology Resilience Principles, requiring firms to define fallback workflows for AI failures such as model degradation or data pipeline breaks.[86] Firms must drill these scenarios regularly alongside traditional outage tests to ensure continuity of critical services.

The EU's Digital Operational Resilience Act (DORA) mandates that financial institutions include AI-specific failure modes in their BCP frameworks. Institutions must document and test fallback options, such as rule-based alternatives or human intervention, for AI component failures and demonstrate readiness through periodic resilience exercises supervised by competent authorities.[87]

Singapore's MAS extends its Technology Risk Management guidelines to cover AI system resilience, requiring firms to predefine backup models or manual processes for drift and API unavailability. MAS expects institutions to conduct integrated BCP drills that simulate both IT infrastructure outages and AI performance failures, ensuring seamless service continuity.[88]

The BIS recommends that central banks embed AI model resilience into their continuity plans, emphasizing scenario-based testing of model drift, adversarial data poisoning, and third-party service disruptions. BIS guidance calls for coordinated drills involving risk, technology, and business units, with documented recovery protocols for AI-dependent functions.[89]

Brazil's Central Bank requires financial institutions to augment their operational resilience frameworks with AI-specific BCP provisions. Firms must establish and test fallback mechanisms such as feature-reduced models or human-in-the-loop processes, for AI failures, reporting drill outcomes to the Centre of Excellence in Data Science and AI and participating in sector-wide resilience workshops.[90]

3.11 AI Incident Reporting and Sectoral Risk Intelligence Framework

Financial sector regulators should establish a dedicated AI incident reporting framework for REs and FinTechs and encourage timely detection and reporting of AI-related incidents. The framework should adopt a tolerant, good-faith approach to encourage timely disclosure.

Regulators should set up a dedicated AI-incident reporting regime, covering both REs and fintechs, to encourage timely detection and disclosure of AI-related incidents (e.g., harmful or biased outputs, model/data compromise, large-scale misclassification, unsafe autonomous actions). Crucially, the

[86]Financial Conduct Authority. (2024, April 22). *AI update: Further to the Government's response to the AI White Paper*. https://www.fca.org.uk/publication/corporate/ai-update.pdf
[87]European Insurance and Occupational Pensions Authority. (n.d.). *Digital Operational Resilience Act (DORA)*. https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en
[88]Monetary Authority of Singapore. (2024, December 5). *Information paper on artificial intelligence model risk management* (ID 18/24). https://www.mas.gov.sg/publications/monographs-or-information-paper/2024/artificial-intelligence-model-risk-management
[89]Bank for International Settlements. (2025, January 29). *Governance of AI adoption in central banks* (BIS Other Paper No. 90) https://www.bis.org/publ/othp90.pdf
[90]Mattos Filho. (2025, May 5). *Brazil's Central Bank presents regulatory priorities for 2025 and 2026*. https://www.mattosfilho.com.br/en/unico/bcb-regulatory-priorities-2025-2026/

Committee advises a good-faith, tolerant approach to first-time reporting to build an open-reporting culture rather than punitive silence. Aggregated, anonymised submissions would feed a sectoral risk-intelligence system for early warning of emerging failure patterns, adversarial campaigns, and concentration risks.

Alignment with the IndiaAI Mission: IndiaAI's ecosystem approach benefits when regulators and firms share structured signals about AI failures and threats. A tolerant, intelligence-oriented incident regime reduces chilling effects on innovation while still surfacing hazards quickly. This complements IndiaAI's Safe & Trusted track and can inform better guidance, datasets (e.g., safety eval corpora), and model cards shared through national platforms.

Global Comparison: The UK's FCA has established structured operational incident reporting frameworks under its Operational Resilience rules[91], with plans to extend these to cover AI-specific incidents through standardized templates and timely disclosure requirements. The FCA emphasizes a good-faith approach to encourage timely reporting and has proposed thresholds for consumer harm, market integrity, and safety concerns, with firms required to provide initial, intermediate, and final incident reports through an online platform.

The EU AI Act mandates comprehensive incident reporting obligations for high-risk AI systems, requiring providers to report serious incidents to market surveillance authorities within 15 days of establishing a link between the incident and the AI system.[92] The Act defines serious incidents to include fundamental rights breaches and requires deployers to immediately inform providers of incidents, with detailed documentation requirements and cross-border reporting obligations across multiple member states where systems are deployed.

Singapore's MAS incorporates AI incident reporting into its existing Technology Risk Management framework, requiring financial institutions to report AI-related incidents as part of their operational resilience obligations.[93] MAS's AI Model Risk Management framework emphasizes continuous monitoring mechanisms and incident response procedures, with specific guidance for managing generative AI incidents and third-party AI system failures through structured governance forums.[94]

The BIS framework recommends central banks establish dedicated AI incident reporting protocols as part of its ten-action governance approach, emphasizing the importance of reporting anomalies and incidents as fundamental to AI risk management. BIS guidance promotes systematic incident documentation, cross-institutional learning, and regular reviews of incident patterns to inform adaptive governance frameworks and risk mitigation strategies.[95]

Brazil's regulatory approach includes mandatory incident reporting through its National AI Regulation and Governance System (SIA), with the National Data Protection Authority coordinating incident responses and sectoral authorities handling domain-specific incidents.[96] Brazil's Central Bank requires financial institutions to report cybersecurity incidents involving AI systems, particularly those affecting payment infrastructure like PIX, with specific obligations for timely notification and recovery efforts, as demonstrated by recent billion-dollar cyberattack responses.

---

[91]Financial Conduct Authority. (2021, March). *Building operational resilience: Feedback to CP19/32 and final rules*. (Policy Statement PS21/3). https://www.fca.org.uk/publication/policy/ps21-3-operational-resilience.pdf

[92]European Parliament and Council. (2024, June 13). *Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689

[93]Monetary Authority of Singapore. (2021, January 18). *Guidelines on Risk Management Practices – Technology Risk*. https://www.mas.gov.sg/regulation/guidelines/technology-risk-management-guidelines

[94]Monetary Authority of Singapore. (2024, December 5). *Artificial Intelligence (AI) Model Risk Management*. https://www.mas.gov.sg/publications/monographs-or-information-paper/2024/artificial-intelligence-model-risk-management

[95]Bank for International Settlements, Consultative Group on Risk Management. (2025, January). *Governance of AI adoption in central banks*. (BIS Representative Office for the Americas, OTHP90). https://www.bis.org/publ/othp90.pdf

[96]Zanatta, R. A. F., & Rielli, M. (2024, December 10). *The Artificial Intelligence Legislation in Brazil: Technical Analysis of the Text to Be Voted on in the Federal Senate Plenary*. Data Privacy Brasil. https://www.dataprivacybr.org/en/the-artificial-intelligence-legislation-in-brazil-technical-analysis-of-the-text-to-be-voted-on-in-the-federal-senate-plenary/

3.12 AI Inventory within REs and Sector-Wide Repository

REs should maintain a comprehensive, internal AI inventory that includes all models, use cases, target groups, dependencies, risks and grievances, updated at least half yearly, and it must be made available for supervisory inspections and audits. In parallel, regulators should establish a sector-wide AI repository that tracks AI adoption trends, concentration risks, and systemic vulnerabilities across the financial system with due anonymisation of entity details.

REs should maintain a comprehensive, up-to-date internal AI inventory covering all models and use cases, data sources/dependencies, intended users/segments, risk tier, performance/monitoring status, incidents/grievances, and owners. Update at least semi-annually and make it available for supervisory inspections. In parallel, regulators should build a sector-wide repository (with entity-level anonymisation) to track adoption patterns, concentration risks (e.g., common third-party models/providers), systemic vulnerabilities, and correlated failure modes across the financial system.

Alignment with the IndiaAI Mission: An auditable AI inventory is the organizational backbone that lets REs safely leverage IndiaAI's public goods (compute, AI Kosh, model/toolkits) and report back on usage and risk. The sector-wide repository reflects IndiaAI's ethos of shared infrastructure and collective intelligence, enabling smarter guardrails and targeted support (templates, evaluations) without exposing competitive secrets.

Global Comparison: The UK's FCA requires firms to maintain detailed AI inventories under its model governance guidelines, including information on model purpose, data sources, performance metrics, risk ratings, and control owners. Firms must refresh these inventories at least quarterly and produce them for thematic reviews and regulatory audits.[97]

The EU AI Act mandates that providers of high-risk AI systems establish and update system registers detailing algorithmic components, training and validation data, performance evaluation results, and human oversight measures. Competent authorities consolidate this information into a central European database to monitor systemic AI adoption and identify concentration risks.

Singapore's MAS requires financial institutions to document all AI use cases, model particulars, dependencies, and risk flags in an AI register aligned with its Model Risk Management framework. Institutions must submit anonymised summaries of this register to MAS biannually to support sector-wide trend analysis and early warning of correlated model failures.[98]

The BIS framework encourages central banks and financial supervisors to develop shared AI inventories at the sector level, anonymising institution-specific details to facilitate cross-border risk intelligence. This repository supports collaborative monitoring of model drift, concentration in third-party AI services, and emerging common vulnerabilities.[99]

3.13 AI Audit Framework

REs should implement a comprehensive, risk-based, calibrated AI audit framework, aligned with a board-approved AI risk categorisation, to ensure responsible adoption across the AI lifecycle, covering data inputs, model and algorithm, and the decision outputs.

[97]Financial Conduct Authority. *AI update*. https://www.fca.org.uk/publication/corporate/ai-update.pdf
[98]Monetary Authority of Singapore. (2024, February). *Information Paper on Artificial Intelligence Risk Management Framework for Financial Institutions*. https://www.mas.gov.sg/-/media/mas-media-library/publications/monographs-or-information-paper/imd/2024/information-paper-on-ai-risk-management-final.pdf
[99]Bank for International Settlements, Consultative Group on Risk Management. (2025, January). *Governance of AI adoption in central banks*. (OTHP90). https://www.bis.org/publ/othp90.pdf

a. Internal Audits: As the first level, REs should conduct internal audits proportionate to the risk level of AI applications.

b. Third-Party Audits: For high-risk or complex AI use cases, independent third-party audits should be undertaken.

c. Periodic Review: The overall audit framework should be reviewed and updated at least biennially to incorporate emerging risks, technologies, and regulatory developments.

Supervisors should also develop AI-specific audit frameworks, with clear guidance on what to audit, how to assess it, and how to demonstrate compliance.

REs should implement a risk-based, calibrated AI audit framework aligned to a board-approved AI risk categorisation and covering the full lifecycle: data inputs and lineage, model/algorithmic design (including training/inference code, features, hyperparameters), testing/validation, performance and drift monitoring, explainability, fairness, and security controls, and decision outputs/business outcomes.

- Internal audits: baseline for all AI, with depth proportional to risk.
- Independent third-party audits: required for high-risk or complex AI.
- Periodic review: at least biennially, to capture new risks, tech, and regulations.
- Supervisors should in parallel publish AI-specific audit expectations, what to audit, how to assess, and how firms should evidence compliance.

Alignment with the IndiaAI Mission: IndiaAI aims for trustworthy, scalable adoption. Audits are the assurance rail that lets REs confidently use domestic models, public datasets, and tools (e.g., AI Kosh) while proving fitness-for-purpose to boards, customers, and supervisors. A formal audit architecture also creates feedback loops into IndiaAI (e.g., common audit findings informing national guidance, benchmarks, and governance toolkits).

Global Comparison: The UK's FCA expects firms to embed AI audit procedures into their existing internal audit functions, with audit scope and depth calibrated to model risk. Internal AI audits must review data lineage, model validation, performance monitoring, and fairness controls, while high-risk applications undergo independent external reviews. The FCA provides detailed guidance on audit methodologies and evidence requirements through its AI and Digital Hub.[100]

The EU AI Act requires high-risk AI systems to be subject to both internal and third-party conformity assessments, effectively serving as audits across the model lifecycle. Providers must maintain up-to-date technical documentation and undergo periodic external evaluations every two years or upon significant changes. Supervisory authorities issue audit guidelines covering data governance, transparency, and post-market monitoring under EBA, ESMA, and EIOPA oversight.

Singapore's MAS mandates AI audit frameworks within its Model Risk Management guidelines. Institutions conduct risk-based internal audits of all AI systems and engage accredited third-party auditors for complex or high-impact models. MAS reviews audit findings during supervisory engagements and updates audit expectations to reflect emerging AI risks and technologies every two years.[101]

The BIS framework promotes a tiered AI audit architecture for central banks and supervisors, recommending a combination of internal audit units for routine checks and independent external experts for high-risk systems. BIS guidance outlines specific audit dimensions, data integrity,

[100]Financial Conduct Authority. (n.d.). *AI update*. http://www.fca.org.uk/publication/corporate/ai-update.pdf
[101]Monetary Authority of Singapore. (2024, February). *Information Paper on Artificial Intelligence Risk Management Framework for Financial Institutions*. https://www.mas.gov.sg/-/media/mas-media-library/publications/monographs-or-information-paper/imd/2024/information-paper-on-ai-risk-management-final.pdf

algorithmic governance, explainability, and security controls, and advises biennial framework reviews to incorporate regulatory developments and technological advances.[102]

Brazil's Central Bank has issued model governance guidelines requiring financial institutions to perform regular internal AI audits and commission third-party assessments for high-risk applications. Audit frameworks must cover data inputs, model validation, drift monitoring, and decision outcomes. The Central Bank consolidates anonymized audit findings to inform sector-wide risk intelligence and updates guidance biennially to capture new regulatory and technological trends.[103]

3.14 Disclosures by REs

REs should include AI-related disclosures in their annual reports and websites. Regulators should specify an AI-specific disclosure framework to ensure consistency and adequacy of information across institutions.

The Committee proposes that REs publicly disclose AI-related information in their annual reports and on their websites. The point is to create comparable, decision-useful transparency across institutions so customers, investors, auditors, and supervisors can understand where and how AI is used, what risks are considered material, what governance exists, and how outcomes are monitored and remedied. The report asks regulators to publish a uniform disclosure framework so that disclosures are consistent, balanced, and not merely promotional. Typical elements would include: AI use-case inventories (at an appropriate level of aggregation), risk-tiering and controls, reliance on third-party models/providers, key consumer-protection safeguards (disclosure of AI use to customers, recourse/complaint volumes and resolution times), significant incidents and remedial actions, and links to model governance policies and board oversight. The idea is not to expose sensitive IP but to standardise the "what stakeholders should know" baseline that is in line with prudential oversight and consumer-protection goals. **Alignment with the IndiaAI Mission:** IndiaAI is designed to scale trustworthy AI through public goods (compute, AI Kosh) and safety-by-design enablers. This recommendation operationalises that ethos by requiring firm-level transparency: REs explain how they use AI sourced or inspired by national platforms, what safeguards they apply, and how customers can seek redress. It also supports IndiaAI's focus on inclusion and accountability. Public disclosures make it easier to detect systemic gaps (e.g., under-served segments, bias in outcomes) and to benchmark sector progress.

Global Comparison: The UK's FCA encourages transparent AI disclosures through its AI Lab initiatives and regulatory principles, asking firms to provide clear information about AI use, risks, controls, and consumer protections in public reports and communications. The FCA promotes consistency via standardized disclosure frameworks aligned with prudential and consumer duty obligations.[104]

The EU AI Act mandates structured AI disclosures for high-risk AI systems, including details on use cases, risk mitigation, governance practices, and incidents. Supervisory authorities require firms to report these disclosures regularly to enable cross-border transparency and informed stakeholder decision-making.[105]

Singapore's MAS integrates AI disclosure requirements within its Model Risk Management guidelines, requiring financial institutions to communicate AI usage, governance controls, and consumer protection

[102]Bank for International Settlements, Consultative Group on Risk Management. (2025, January). *Governance of AI adoption in central banks*. (OTHP90). https://www.bis.org/publ/othp90.pdf
[103]Southard, J. (2024, December 13). *Banco Central do Brasil launches data science and AI centre of excellence*. Global Government Fintech. https://www.globalgovernmentfintech.com/banco-central-do-brasil-centre-of-excellence-data-science-ai/
[104]Financial Conduct Authority. (n.d.). *AI update*. http://www.fca.org.uk/publication/corporate/ai-update.pdf
[105]European Parliament and Council. (2024, June 13). *Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689

measures on public platforms. MAS supports sector-wide frameworks to harmonize disclosures and enhance trust in AI deployment.[106]

The BIS advocates for sector-wide transparency supported by audit trails and public reporting of AI governance outcomes. Its guidelines encourage financial supervisors to mandate AI disclosures that balance transparency with confidentiality, contributing to more robust systemic risk monitoring.[107]

Brazil's Central Bank requires AI disclosures aligned with governance and consumer protection mandates. It guides institutions on public communication of AI use, risk management efforts, and incident resolution, supporting regulatory oversight while safeguarding competitive interests.[108]

3.15 AI Toolkit

AI Compliance Toolkit will help REs validate, benchmark, and demonstrate compliance against key responsible AI principles such as fairness, transparency, accountability, and robustness. The toolkit should be developed and maintained by a recognised SRO or industry body.

The Committee recommends an AI Compliance Toolkit, maintained by a recognised SRO/industry body, to help REs validate, benchmark, and evidence compliance against the core principles of responsible AI across the model lifecycle. Concretely, the toolkit would provide:

- Checklists & templates (model cards, data lineage logs, bias & explainability reports, human-in-the-loop thresholds, change-control records).
- Metrics & tests for fairness and drift, robustness/adversarial testing harnesses, explainability artefacts, and red-team playbooks aligned with sectoral risks.
- Reference evaluations/benchmarks and calibration guidance for key financial use cases (e.g., credit underwriting, fraud, AML screening, collections), plus audit-ready evidence packs. A shared toolkit reduces compliance burden, levels the playing field for smaller REs, and increases comparability of what "good" looks like during supervisory reviews and third-party audits.

Alignment with the IndiaAI Mission: IndiaAI supplies public rails in the form of datasets via AI Kosh, compute access, and a national focus on Safe & Trusted AI. The Toolkit is the enterprise-level adapter: it converts those rails into repeatable artefacts and proofs that REs can attach to product approvals, audits, and disclosures. This is especially important for MSMEs and smaller REs, who gain ready-to-use fairness/robustness test suites and documentation scaffolds without building everything from scratch, directly advancing IndiaAI's democratisation and safety aims.

Global Comparison: The FCA's approach is highly collaborative, using initiatives like TechSprints and its AI Lab to bring together regulators, firms, and academia.[109] While not a single, prescribed "toolkit," these efforts result in shared insights, prototype tools, and best practices. The FCA's focus is on ensuring firms apply existing regulatory principles (like the Senior Managers & Certification Regime) to their AI models, emphasizing robust governance, explainability, and consumer protection.[110] The goal

[106]Monetary Authority of Singapore. (2024, December 5). *Artificial Intelligence (AI) Model Risk Management*. https://www.mas.gov.sg/publications/monographs-or-information-paper/2024/artificial-intelligence-model-risk-management
[107] Bank for International Settlements, Consultative Group on Risk Management. (2025, January). *Governance of AI adoption in central banks*. (OTHP90). https://www.bis.org/publ/othp90.htm
[108]Mattos Filho. (2025, April 24). *Central Bank of Brazil announces Regulatory Priorities for 2025-2026*. https://www.mattosfilho.com.br/en/unico/bcb-regulatory-priorities-2025-2026/#:~:text=On%20April%2024%2C%202025%2C%20the,the%20expansion%20of%20Pix's%20functionalities.
[109]Henderson, A., Barwick, G., Scott, G., Taylor, J., & Dixon-Ward, M. (2024, April 25). *The FCA's AI update: Integrating the UK Government's 5 principles*. Goodwin Procter. https://www.goodwinlaw.com/en/insights/publications/2024/04/alerts-finance-aiml-the-fca-ai-update
[110]Financial Conduct Authority. (2025, September 9). *AI and the FCA: Our approach*. https://www.fca.org.uk/firms/innovation/ai-approach

is to facilitate safe innovation by creating a testing environment (sandboxes) and encouraging the development of practical tools.[111]

The EU AI Act mandates detailed disclosures for high-risk AI systems, including AI inventories, risk controls, third-party dependencies, incident reporting, and governance oversight. Regulators require firms to report regularly, ensuring cross-border transparency and enabling stakeholders to make informed decisions about AI use in financial services.

Singapore is a leader in this area with its Veritas Toolkit. Developed by an MAS-led consortium of over 30 industry players, Veritas is an open-source toolkit designed to help financial institutions assess their AI solutions against the MAS's principles of Fairness, Ethics, Accountability, and Transparency (FEAT).[112] The toolkit provides practical methodologies and code libraries to evaluate AI models for bias, explainability, and accountability, thereby lowering the barrier for smaller firms to adopt responsible AI practices.[113] This is a prime example of a regulator and the industry collaboratively building a shared resource to ensure trust and compliance

The BIS, through its Innovation Hub, is actively exploring the use of AI for supervisory purposes (SupTech). Its projects, like Project AISE (Artificial Intelligence Supervisory Enhancer), aim to create an AI-driven toolkit to help financial supervisors manage the growing complexity of regulatory oversight. The BIS's work focuses on providing a framework and technical solutions that can be adopted by central banks and regulators globally to enhance their oversight capabilities, complementing the toolkits used by firms themselves.[114]

While Brazil's AI regulatory framework is still taking shape with a new AI bill (Bill No. 2,338/2023) recently approved by the Senate, the BCB's approach is centered on ensuring that institutions have the necessary governance and controls in place.[115] The BCB expects financial institutions to manage AI risks effectively, aligning with its existing data protection and cybersecurity rules. The BCB has created a Center of Excellence for Data Science and Artificial Intelligence to develop new technologies and foster the use of AI within the agency, providing guidance for the safe and ethical use of AI.[116] This internal focus on governance sets a precedent for the expectations it will place on supervised institutions, compelling them to create their own robust "toolkits" of policies and procedures.

[111]Financial Conduct Authority. (2025, May 14). *AI Sprint summary*. https://www.fca.org.uk/publications/corporate-documents/ai-sprint-summary
[112]Dimitrov, M. (2025, July 3). *Singapore's MAS launches Veritas Toolkit 2.0 for responsible AI in FinTech*. FinTech Global. https://fintech.global/AIFinTechForum/singapores-mas-launches-veritas-toolkit-2-0-for-responsible-ai-in-fintech/
[113]Monetary Authority of Singapore. (2023, June 26). *MAS-led Industry Consortium Releases Toolkit for Responsible Use of AI in the Financial Sector*. https://www.mas.gov.sg/news/media-releases/2023/toolkit-for-responsible-use-of-ai-in-the-financial-sector
[114]Bank for International Settlements. (2024, November 19). *Innovation and AI*. BIS. Retrieved September 18, 2025, from https://www.bis.org/topic/fintech/innovation_ai.htm
[115]Mattos Filho. (2024, December 11). *Regulatory framework for artificial intelligence passes in Brazil's Senate*. Retrieved September 18, 2025, from https://www.mattosfilho.com.br/en/unico/framework-artificial-intelligence-senate/
[116]Faridi, O. (2024, September 14). *Banco Central do Brasil (BCB) Accelerates Introduction of AI into Business Processes*. Crowdfund Insider. Retrieved September 18, 2025, from https://www.crowdfundinsider.com/2024/09/230020-banco-central-do-brasil-bcb-accelerates-introduction-of-ai-into-business-processes/

4. Practical Implications for Indian Banks & Fintechs

The FREE AI recommendations surpass existing RBI and SEBI rules to introduce novel operational obligations for all Indian financial firms. While current regulations cover credit risk models, outsourcing, and algo-trading safeguards, they were largely ignorant of AI-specific risks such as bias, explainability, or systemic concentration.

Key additions include a full AI inventory across all departments of fraud engines, chatbots, vendor APIs, marketing tools and so on. Free AI scales the existing board-approved policy requirement to explicit AI oversight including bias checks, red-team results, and fairness KPIs. It extends the internal audits system to adversarial testing (e.g., prompt injection, fake KYC inputs) and fairness audits. BIS's diversification recommendations echo in the report's call for participation in shared repositories and adoption of indigenous Indian-developed models.

These recommendations aspire to cumulatively propel Indian banks to treat AI governance as a board-level compliance item and not a mere technical IT function, additionally expanding the perimeter of regulatory expectations.

4.1 Equitable Access to High Quality Data

Though directed primarily at regulators as well as industry bodies, REs will not fail to feel the operational effects of this recommendation because they will have to contribute and consume data. Calling for the creation of digital public infrastructure for our financial sector, linking it to AI Kosh, so high-quality anonymised datasets can be shared and deliberated upon. For REs, this might mean setting in place linear pipelines to extract data, remove all personal information, apply anonymisation/ privacy-enhancing technologies and then upload this processed data in standard formats defined by respective industry bodies or SRO. Dedicated data engineers, privacy officers, and legal staff have to work together to prep and verify such contributions. Industry bodies set templates and APIs for submission, REs keep logs, dataset manifests, and audit trails of each and every contribution. Practically speaking, this could involve quarterly/ semi-annual dataset submissions with alerts for failed uploads or rejected files and systems will need to support secure transfer, plus staging of sandboxes to validate data before it is shared online. This marks a systemic shift towards treating anonymised financial data as a shared public good, REs are expected to play an active role in both contribution and benefiting from this infrastructure.

4.2 Capacity Building and AI Governance

Aimed at SROs and industry bodies, they are expected to set all sector-wide registries and mechanisms up so as to sharing incidents, tracking vendor concentration, and running stress tests. For REs this creates indirect yet significant obligations since they have to supply regular feeds of information to the sector registry including inventories of AI models in use, vendor dependencies such as cloud or foundation model providers, and incident summaries. For this, REs will need to map their internal systems in relation to common taxonomies and identifiers provided by the SRO, then the data can be aggregated and compared across sectors. Coordination groups or working committees will have be formed and REs will have to designate senior risk or technology officers to represent them and share experiential lessons. With time this will translate to producing anonymised incident reports, tagging models with standard risk classifications, and providing metrics that can feed into collective stress-testing. Thus while SROs manage the registry and coordination, the burden on REs will entail continuous reporting, standardisation, and active participation.

4.3 Board-Approved AI Policy

Directly targetting REs and requiring them to adopt a comprehensive board-approved AI policy under which the policy must cover governance, accountability, risk appetite, lifecycle management, disclosures, consumer protection, auditability, and liability. Industry bodies have a supportive role in publishing template policies that smaller REs can adapt going forward. Operationally, this will elevate AI oversight from being just a compliance or IT matter to something that boards themselves must own and be accountable for. They will need to schedule regular briefings on AI risk, maintain minutes accounting their decisions and demonstrate active oversight of fairness, accountability, and transparency undertaken by them. REs will create clear roles such as AI risk owners, model risk leads, and data stewards, also reporting lines up to the board. Evidence packs will be expected for pre-approvals, for example, inventories of models, audit reports, or results from red-team testing; and form part of the board's decision-making records. For smaller REs, templates from industry bodies will reduce the drafting burden, still leaving them the need to integrate this policy into their operations.

4.4 Governing the AI Data Lifecycle

Placing responsibility on REs to arrange robust data governance for AI. This requires controls over the entire data lifecycle, right from collection and storage to use, retention, and deletion, with privacy-enhancing technologies wherever and whenever appropriate. For operations, this implies REs maintain an enterprise data catalog that records the origin of data, how it is transformed and what it is used for and its consequent retention and current consent status. Tools like metadata managers and lineage trackers become part of this compliance stack. Every change applied to a dataset such as schema adjustments or enrichment have to be logged and reversible. Privacy officers will need to carry out regular and frequent impact assessments and record the rationale for using techniques like differential privacy, synthetic data, or federated learning. Model training is gated by data quality checks and steward approvals, so models may not proceed if data fails bias thresholds or completeness standards. This shifts day-to-day working style by making data stewardship a central tenet of AI operations inside REs.

4.5 AI System Governance Framework

This recommendation applies to REs and proclaims governance of AI systems from the very start to the very finish, including its design, validation, deployment, monitoring, and retirement. Operationally, REs must set up a central model registry whose job is to record every detail about each AI system: the data it was trained on, the code and parameters used, the owner,and the last validation date. Each deployment is followed by a package of documentation that includes validation results, fairness metrics, cybersecurity assessments, fallback plans, and approval sign-offs. Once in the middle of production, models are to be continuously monitored for drift, latency and fairness issues, with automated alerts on detection going directly to risk and model operations teams. Retirement procedures must also be formalized so the models that are no longer valid are archived with their training data, code snapshots, and explanations for why they were decommissioned suddenly. This makes AI governance a continuous, documented process rather than a one-time activity.

4.6 Product Approval Process

This recommendation requires all REs to embed AI risk assessments intimately and inherently into the approval process for any new financial product that uses AI. The impact on operations is that product sign-off templates will then also include a dedicated section on AI. Business teams will need to explain what the AI does, what data it uses, how tests for fairness and robustness are conducted and what fallback options do exist if the AI ever fails. Independent risk and compliance reviewers are independent of developers, and will gain veto powers over whether the product can be taken forward. Evidence such as back-testing results, customer impact assessments, and human review protocols will all become mandatory attachments to every product proposal. This will ultimately slow down time-to-market ratio

but also ensure risks are crucially identified and proactively addressed very early on in the product lifecycle.

4.7 Putting Consumers First

Due to this recommendation REs are obliged to create a board-approved consumer protective framework for AI. This will require higher commitments on transparency, recourse, education, and monitoring of disparate impacts on their end. Operationally, REs would need to publish disclosures in a simplistic language explaining how AI decisions are made, for example- in loan approvals or fraud detection. Customer service teams will have to be retrained to handle variegated queries and appeals considering AI decisions, done through standardised scripts and forms. Complaints will be logged and monitored under the keen eye of new key performance indicators such as time to resolution or the rate of human overrides of AI decisions. In addition, REs should be running consumer education and awareness campaigns through specialised websites, apps, or public outreach to explain how AI is used in financial services simply. All these activities are to be recorded and versioned so as to demonstrate dedicated compliance to the recommendation.

4.8 Mitigating Cybersecurity Threats

This recommendation requires REs to accommodate AI- specific risks like data poisoning, prompt injection, or model theft under their cybersecurity practices to develop combatting frameworks. In practice, this will intend extension of existing threat modelling exercises so they include AI endpoints and training pipelines. System design documents will need to identify risks like adversarial inputs or exfiltration of training data. Security teams will have to undertake adding runtime protections like input sanitisation, anomaly detection, and rate limits for all model APIs. Monitoring systems must be capable enough to detect and report suspicious activity linked to AI usage, for eg. repeated manipulation attempts. Incident response playbooks must outline AI-specific scenarios and then should be tested for effectiveness and efficiency in drills. Clauses covering these risks should be included in procurement contracts for third-party AI providers. In short, cybersecurity in REs will no longer be only about IT network systems but go beyond that to the AI models themselves.

4.9 Red Teaming of AI Models & Applications

This recommendation requires all REs to start out with adversarial testing of AI systems in proportion to the inherent risk they pose. Operationally, REs will need to create the frameworks for formal red-teaming programs with a clear delineated schedule, for example monthly tests for high-risk models and quarterly tests for medium-risk ones. The red-team exercises should include but not be limited to prompt injection, adversarial inputs, distributional shifts, and bias exploitation. Reports from these respective exercises will need to document all the scenarios that have been tested, the vulnerabilities that have been found and the remediation steps taken pronto, with deadlines for fixes in great detail. Procurement policies will also need to be amended with third-party vendors now required to allow red-teaming of their systems and to further cooperate in fixing the issues that come up. These processes will make adversarial testing a routine and auditable part of the AI lifecycle in REs and revolutionise it.

4.10 Business Continuity Plan for AI Systems

REs are to extend their business continuity planning (BCP) to cover AI failures, following this recommendation. For operations, this will mean identifying each critical AI function and then designing relevant fallback mechanisms such as manual reviews or rule-based alternatives. Playbooks will need to be descriptive with step-by-step of how staff should act when an AI system fails including escalation contacts and override procedures, that don't leave any doubts. Staff must also be trained to handle these fallbacks with regular drills to test their proactivity and readiness. Other defining and monitoring will cover metrics such as recovery time objectives (RTO) and recovery point objectives (RPO) for AI systems. All these steps ensure that financial services can continue even when AI tools suddenly stop

working, but it will require a significant amount of planning, rigorous staff training and ample resources on hand.

4.11 Incident Reporting and Risk Intelligence Framework

This recommendation creates further new obligation for REs to report all AI-related incidents to either regulators or SROs. Operationally REs will have to classify such incidents according to a few standard categories like bias events, security breaches or major system errors, and so on to prepare anonymised reports for submission. To feed monitoring data directly into reporting systems, automated pipelines will likely have to be built with strict deadlines for initial notification (for example, 48 hours after discovery). Compliance teams will need to amp up to monitor AI systems continuously for reportable incidents and furthermore, internal escalation procedures will need that the right people are informed quickly and called in for resolution. Once incidents are reported sector-wide intelligence may then go back from regulators/SROs, requiring REs to include detection rules and security measures under its ambit. This makes dynamic incident reporting both a compliance duty and a source of evolving ongoing sectoral learning.

4.12 AI Inventory and sector-wide repository

This recommendation requires REs to maintain an internal inventory of all AI systems, and SROs to maintain a sector-wide anonymised repository. Operationally, REs must note for every AI model: its name, purpose, owner, inputs and outputs, vendor, hosting environment, risk tier as well as validation history. These inventories must be current and auditable, regularly updated and thus always ready for inspection during sudden regulatory reviews. To allow regulators to compare across time, historical data and snapshots are also to be archived. SROs will have to run repositories that collect and account for anonymised data from all REs at a sector-wide level. Therefore REs will need to keep mapping and syncing their internal identifiers to sector level standard IDs so consistency is maintained and performed. This adds a layer of ongoing reporting and integration work and therefore gives both regulators and industry a clearer picture of systemic AI use.

4.13 AI Audit Framework

This recommendation needs REs to subject all AI models to risk-based audits with high-risk models undergoing independent third-party reviews too. Operationally, this will mean that internal audit teams do expand their scope to cover AI lifecycle risks including data inputs, code, fairness tests, and security posture. Validation reports, training data attestations, red-team results, and remediation logs are all credible audit evidence. Audits should produce formal ratings and corresponding timelines for corrective actions, all continuously tracked by compliance teams. REs will also need external AI auditors for the most critical of their models, this adds cost but also strengthens credibility with supervisors simultaneously. Industry bodies or SROs maintain certified auditor registries for standardised quality. This will equalise the level of scrutiny imposed on AI and financial risk models.

4.14 Disclosures by Regulated Entities

Customers and regulators need structured disclosures about AI use by REs, under this recommendation. In practice, this means disclosure templates to be made that describe what the AI does, what various factors it considers and how customers can appeal their decisions too. These disclosures must be in plain language and updated whenever changes are brought about in the model. REs keep records of all these required disclosures with respective timestamps and versions, this way supervisors can easily verify compliance too. To handle queries triggered by disclosures adequately, customer service operations will need to evolve, appeals will need to be processed within defined service levels. This may increase the volume of disputes that arise subsequently but will also improve consumer trust in

the system. For regulators, these disclosures provide transparency into how AI is transforming the financial services and aligning India with standards prevalent globally.

5. Way forward

The FREE-AI committee report marks a pivotal moment in India's regulatory journey at the intersection of artificial intelligence and financial services. By establishing a detailed framework spanning across capacity building, data governance, cyber security, and AI-audit the Reserve Bank of India positions India among a handful of jurisdictions that are looking to proactively address the duality of AI-driven innovation and risk mitigation arising out of the application of this layer of technology.

The approach of the committee has been methodical, context-aware, and forward looking in its outlook. Their recommendations are closely benchmarked against leading international best practices namely the UK's tiered risk regime, Singapore's collective capacity-building, UK's principle-based approach and Brazil's light touch innovation fostering regulations. Yet, the FREE-AI framework remains rooted in Indian realities and aligns well with the IndiaAI Mission, the DPDP Act and the overarching need for indigenous AI capabilities. Its emphasis on board-level accountability, robust data lifecycle governance, consumer protection and creation of digital public infrastructure sends the right signals over a medium and long term timeline.

The report does well to highlight the operational and implementation hurdles that players of varying size and business models will face. The proposed expansion of compliance parameters including but not limited to inventorying AI models, third party audits, and red-teaming exercises involve significant investments in talent and technology, more so for smaller regulated entities. The demand for sector-wide information sharing, structured disclosures and AI incident reporting will have to be balanced alongside concerns of privacy, market competition, and standardisation.

Going forward the key challenge for the Indian financial sector institutions will be to translate the recommendations into practice such that it balances innovation with risk mitigation as envisaged. Towards that end the industry will expect future regulatory guidance in this space to be adaptive, phased, sandboxing focused, and inclusive of new learnings from local and global experiences. Successful adoption of AI in the sector will rely on regulatory clarity as with industry investment in capacity augmentation and standard development. If the zeal of the report is manifested in its implementation, the FREE-AI framework can serve as a model for responsible AI adoption in other domains within the financial sector. The way forward will underscore how we advance our strategic ambitions while safeguarding the interests of consumers and protecting the stability of the broader financial system.

Authors

Soham Jagtap

Senior Research Associate, The Dialogue

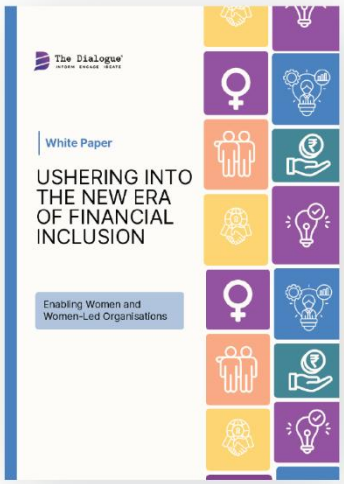
Soham Jagtap is a Senior Research Associate, at The Dialogue, focusing on AI and data protection. Instead of e-commerce and fintech. He holds an LLM in Law and Technology from NUJS, where he graduated with the highest distinction in 2023. His research explores the intersection of law and technology, with work spanning AI ethics, fintech policy, and justice delivery through technology. At The Dialogue, Soham contributes to shaping policies that balance innovation and public interest through rigorous legal research and analysis.

Ranjeet Rane

Partner, Fintech & Sustainable Finance, The Dialogue

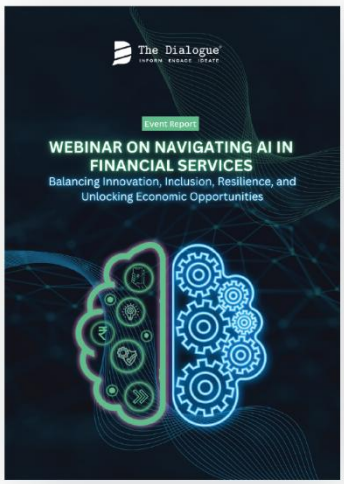
Ranjeet Rane is Partner at The Dialogue, where he leads the Fintech and Sustainable Finance verticals. A public policy professional with over 15 years of experience in tech policy, fi nancial regulation, and digital innovation, he previously led policy research at RBIH and ReBIT. Ranjeet is a PhD scholar, amateur birder, and longtime advocate for responsible innovation in India's digital economy.

More from our Research



WHITE PAPER

Ushering into the New Era of Financial Inclusion: Enabling Women and Women-Led Organisations



EVENT REPORT

Webinar on Navigating AI in Financial Services – Balancing Innovation, Inclusion, Resilience, and Unlocking Economic Opportunity

RESEARCH PAPER

Digitising India: Towards an Inclusive Growth of the Ecosystem

POLICY BRIEF

The 25th Report of the Parliamentary Standing Committee on Finance

thedialogue.co

@_DialogueIndia

@TheDialogue_Official

@The-Dialogue-India

@TheDialogue