TATA CONSULTANCY SERVICES

Building on belief

Augmenting the reliability and fairness of AI in financial services

Abstract

The growing reliance on artificial intelligence[1] (AI) technologies has led to its rapid adoption across several functional domains in the financial services sector. While bringing significant business benefits and potential for innovation, AI has also added new dimensions of risks. Besides data privacy and security-related vulnerabilities, the prevalent lack of transparency in AI systems demands increased accountability and governance. With less-explainable and unfair outcomes that can create bias in models, global regulators recognize the black-box nature of risks posed by automated decision systems that can aggravate systemic impacts in the absence of sufficient governance mechanisms.

Regulatory formulations aimed to create governance standards and guidelines for managing AI risks are currently underway in different jurisdictions. As a part of their AI strategies, banks need to evaluate inherent risks and establish well-defined policies and governance frameworks to augment the transparency and reliability of AI systems. This white paper outlines how a robust governance framework can help banks harness the true potential of intended business benefits while prudently managing the associated risks.

AI: Propelling business innovation and efficiency in financial services

Given the prevalence of data and intelligence-driven ecosystems, financial institutions have been actively adopting AI and machine learning (ML) in diverse areas of their business. These include customer-focused products and services; customer profiling; risk management and capital allocation; investment and trading; regulatory compliance, as well as a few non-conventional areas such as data quality monitoring and document interpretation. When it comes to business innovations and productivity gains, AI is used in credit approval, product recommendation, product pricing, risk modeling, fraud detection, know your customer (KYC), anti-money laundering (AML), and regulatory data reporting, among others.

[1] *The term 'artificial intelligence (AI)' in this paper recognizes all associated cognitive and self-learning technologies – including machine learning (ML), natural language processing (NLP), and voice recognition among others.*

Assessing the risks involved in automated decisions systems

While AI use cases promise significant innovation and opportunities for efficiency, it brings new vulnerabilities and unconventional risks such as inaccurate credit scores, improper product recommendations, denial of service, discriminatory pricing, and so on. The nuances of AI risks are hard to predict, interpret, and control immediately. If not sufficiently addressed, these risks can lead to unexpected consequences, both at the bank and the financial system level. Self-learning and adaptive methods may introduce discriminatory bias driven by age, gender, race, or social behavior patterns in models, due to lack of proper design and validation, and cause unfair and inequitable outcomes. AI risks are less obvious, hard to audit, and have limited explainability, and can therefore exacerbate data privacy, security, model governance, and third-party related risks.

As definitions and standards of risk categorization, risk mitigation, and governance norms evolve in the industry, newer dimensions of risks inherent to AI systems emerge across their lifecycle (see Figure 1).

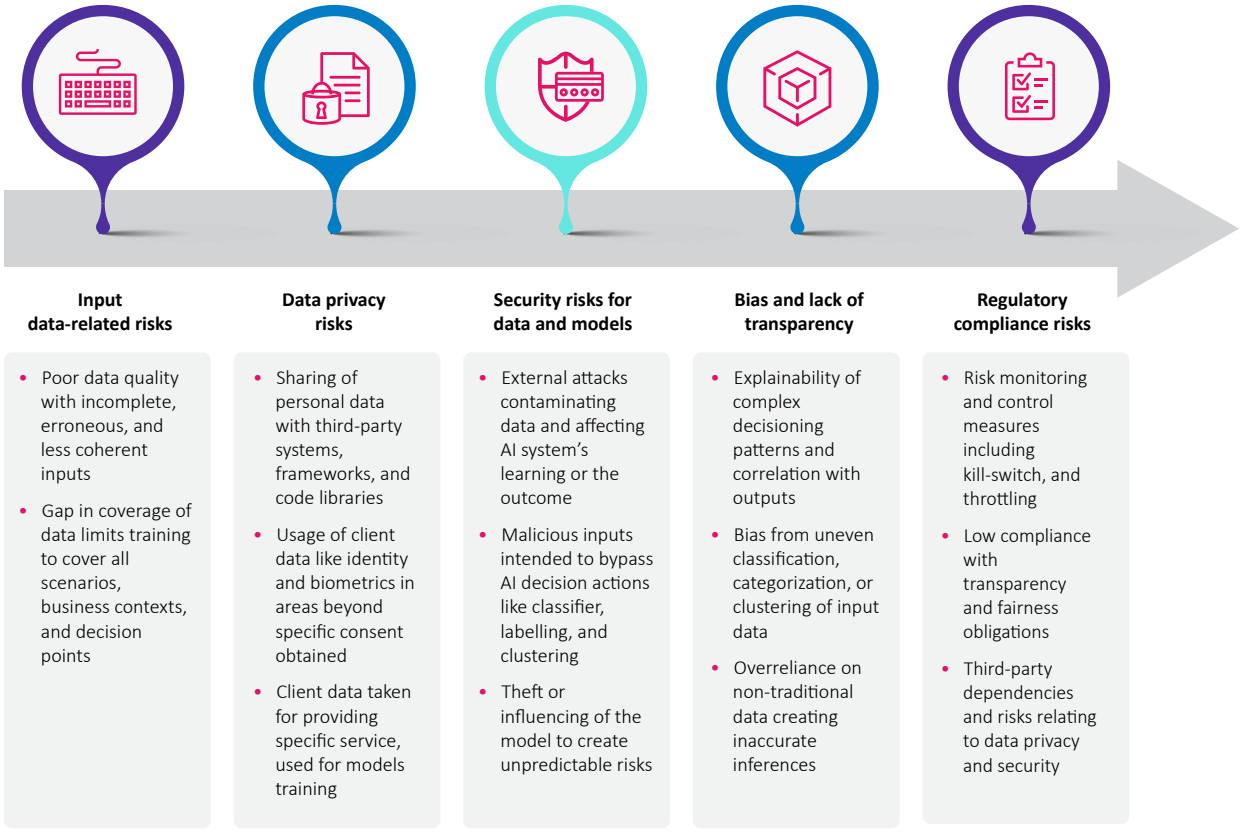

Figure 1: Risks involved in automated decisions systems

Emerging regulatory standards and frameworks

Considering the unpredictable nuances of risks involved in AI systems, regulatory focus primarily hinges on balancing the twin policy priorities of fostering innovation and technological advancements in the industry and ensuring sound and responsible adoption of technological capabilities to avoid potential systemic impact. Ensuring customer protection through fair and transparent decisions and safeguarding data privacy and cybersecurity become equally important considerations.

In recent times, global regulators have been formulating standards to establish accountability and governance for the prudent use of AI systems. The EU Harmonized Rules on AI, the UK ICO's Guidance on the AI Auditing Framework, the US Federal Trade Commission's Guidelines on Truth, Fairness, and Equity in the use of AI, and Singapore's Model AI Governance Framework are some of the notable regulatory frameworks. Their objective is to institutionalize a holistic governance framework encompassing the AI system and its functioning across the lifecycle - design, development, validation, and monitoring.

Business adoption of AI use cases: Key impact for financial services firms

Financial institutions' AI adoption journey is largely driven by their business model, customer segment focus, product portfolio, and regulatory status, besides innovation ambitions. The proliferation of data (traditional and non-traditional) and the resultant mining of business insights and intelligence have accelerated the adoption of AI across a wide spectrum. Financial institutions must gain a broad-level understanding of AI-centric use cases in their specific business context, their adoption level along with associated risks, and degree of impact across key risk dimensions (see Table 1).

Functions	AI dimension or maturity	Potential risk impact	Risk factors				
			Input data related risks	Data privacy risks	Security risks for data and models	Bias and lack of transparency	Regulatory compliance risks
Client onboarding: KYC, AML, and due diligence	Predictive and prescriptive	Higher false positive and true negative cases, biased inferences, and incoherent noise	Limited training data coverage	Leakage of client sensitive data	Cybersecurity and malicious threats of affecting data and model functioning		Low data quality and auditability
Credit appraisal: Credit scoring, loan approval, and pricing	Predictive	Incorrect categorization, imprecise credit and risk assessment, discriminatory pricing, and service level	Undue weight to non-traditional data	Data sharing with third parties		Uneven clustering with skewed interpretation	Limited explainability of outcomes
Client risk monitoring: Fraud detection, default prediction, and early warnings	Predictive	Higher false positive and true negative cases, biased inferences, and incoherent noise	Limited training data coverage	Data sharing with third parties		Misconceived cues guiding pattern deduction	Low data quality and auditability
Algorithmic trading and investment strategies	Predictive and prescriptive	Uncontrolled trading behavior and wide-market impacts	Low training on dynamic data			Complex learning of algorithms and threshold setting	Missing controls – kill switch and throttling
Investment advisory	Prescriptive	Incorrect categorization, biased recommendations with product knowledge and risk-mismatch	Limited training data coverage	Usage of data beyond consented area		Imprecise decision of risk appetite and product knowledge	Limited transparency for client interests
Risk management and capital provisioning	Predictive and prescriptive	Unpredictability in dynamic scenarios, low reliability of modeling outcome	Imprecise interpretation of past trends			Disproportionate weight to tail risks	Low correlation and traceability of outcomes
Compliance: Regulatory data reporting and trade surveillance	Prescriptive	Imprecise rules interpretation and missing Interconnectedness	Non-harmonized data limiting linkages				Low data quality and auditability
Client services	Prescriptive and predictive	Preconceived response levels with profiling bias and overlooking human emotion	Low training for human context	Usage of data beyond consented area		Risk of manipulation of human interaction	Lower explainability of outcomes

High impact Moderate impact Basic or low impact

Table 1: Key use cases and impact across risk dimensions

AI risk governance: How can financial institutions establish a sustainable framework?

Against the backdrop of evolving regulatory standards in the financial services industry, an enhanced governance framework for oversight of potential risks from AI systems is crucial in order to improve accountability, auditability, and transparency levels. As part of firms' AI-centric programs, a few critical imperatives need to be addressed on priority to holistically fulfill regulatory obligations. The imperatives include establishing appropriate risk management and control measures, policy and procedures, data governance, documentation, and record-keeping norms, alongside procedures for human oversight and transparent information to users (see Figure 2).

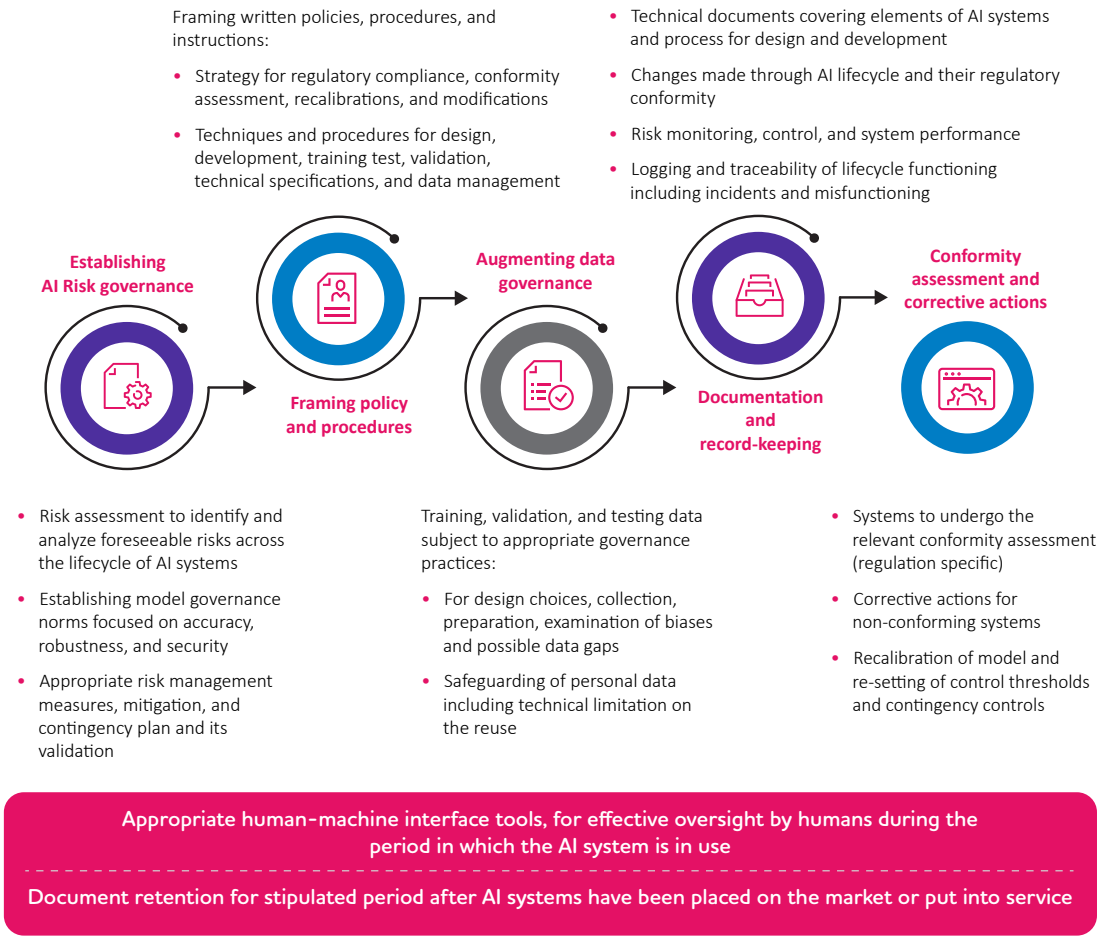

Figure 2: AI risk governance: Key imperatives

Priorities of an AI risk governance framework

Financial institutions' AI risk governance model and supervision framework rests on the key pillars of people, process, and technology with distinct focus areas (see Table 2).

Focus areas	People	Process	Technology
Risk management policies and practices	Oversight and knowledge among senior management, contextual knowledge of AI model objectives, outcomes, and risks	Safeguarding customer rights; model outcomes in-line with defined objectives; identifying risk scenarios, mitigation measures, and contingency controls, AI remediation and recalibration	Evaluating third-party risks, model design-related limitations and addressing inherent biases, model security and missing or non-synchronized data handling
Model risk governance and lifecycle management	SME knowledge about model objectives, outcomes, and risks, model alignment with compliance standards, accountability, and coordination between involved teams	Model or algorithm selection – supervised, unsupervised, reinforcement or transfer learning; AI model development processes and quality outlier handling; training and testing data coverage and consistency	Architecture and components landscape, technology patterns, modern technology considerations, infrastructure provisioning, versioning, and documentation controls
Data governance and control	Stewardship, roles, and responsibilities	Data policies and standards, data quality, validation, and remediation process; PII data handling and consent management; metadata and lineage	Data governance platform and supervision capabilities, data quality solution, data privacy protection capabilities
Operational supervision	AI model impacts on stakeholders, operational controls and monitoring, alerts for deviation in model output	Assessments and audits; human intervention and review for high-risk areas; contingency measures and AI remediation; continuous monitoring	Monitoring of outcomes for trend analysis, human interface and review features, collaboration platform

Table 2: Key priorities of AI governance framework

AI risk governance model

Establishing and enabling a governance foundation with guiding principles and control thresholds across key dimensions becomes a basic requisite for the optimized functioning of AI systems. A robust AI risk governance framework involves oversight of the AI model lifecycle, enterprise policies, and data governance norms across all the AI programs. To align with regulatory frameworks, the governance framework should spell out clear objectives, guidelines, and standard criteria for model adoption processes, monitoring, and control, besides data and model security aspects.

Resilient model governance and procedures covering functions like model validation, model quality testing, model monitoring, model output analysis (explainable outcomes), and trends need to be outlined. To avoid known or unknown risks and mitigate their unwanted consequences, the model governance guidelines must consider business objectives, decision consequences, data patterns, testing adequacy, data privacy, and security aspects.

In terms of cybersecurity, the governance framework must consider risk scenarios across model and data protection, model extraction attacks, and training data poisoning. Additionally, laying down overall assessment and audit processes is critical to swiftly identify and remediate gaps. To drive the well-tuned functioning of AI governance, business groups should closely work with data governance teams and ensure that data quality, metadata management, and data traceability norms are fully adhered to.

Augmented data governance for de-biasing and improved accountability

Data being the most critical element in the design of AI models and their training, the effectiveness of an AI system is completely dependent on sound data quality and a governance framework. Augmented data governance processes can boost the learning capability of AI models and eliminate data-induced biases to produce fair and consistent outcomes. This necessitates a drastic shift in key

dimensions of data management processes for effective planning, provisioning, and accessibility of requisite datasets across the AI lifecycle. These dimensions include:

- Data coverage: Usage of full or partial synthetic data to extend conditions variability, undiscovered scenarios, and outliers' coverage.
- Data quality: Automated monitoring, remediation, and dashboarding for aberrations and unusual patterns.
- Data traceability and control: Establishing lineage of data used in training, testing, and validation. Metadata management can identify the source and context efficiently.
- Data protection: Simulated and synthetic data creation for the training and testing of AI models to overcome data usage restrictions.

Conclusion

AI adoption is fast emerging as a strategic imperative for financial institutions, given its ability to help tailor personalized customer experience. In addition, as banks move to ecosystem business models, reliance on AI to unlock the power of data insights from varied sources will only increase. However, AI risks pose complex challenges; to overcome them, financial institutions must ensure that AI systems comply with evolving regulatory guidelines as well as risk management standards and tolerance limits. To this end, financial institutions must establish a foundational AI framework with robust governance to exploit AI-led innovations, gain an edge in the market, and march ahead of the competition.

About the authors

Indra Chourasia is an industry advisor in the Chief Data Officer (CDO) Strategic Initiative group of the Banking, Financial Services, and Insurance (BFSI) business unit at TCS. With over 25 years of global experience in business and IT advisory and implementation projects, he designs solution offerings and drives thought leadership and client engagements in capital markets. Indra has a Bachelor's degree in Civil Engineering from Nagpur University, India, and a Master's degree in Financial Management from Magadh University, India.

Sivagurunathan Ranganathan is a chief architect in the Chief Data Officer (CDO) Strategic Initiative group of the Banking, Financial Services, and Insurance (BFSI) business unit at TCS. With over 23 years of experience in the data and analytics domain, he is involved in consulting, architecting solutions, and implementing large programs for global banks and insurers. He has a Bachelor's degree in Electronics and Communication Engineering from Madras University, India, and an MBA from Annamalai University, India.

Prab Pitchandi is the global head of Chief Data Officer Initiatives in the Banking, Financial Services, and Insurance (BFSI) business unit at TCS. He has over 25 years of experience in the BFSI space. In his current role, he works with financial services institutions to enable them to become data-driven organizations, create an automated and contextual data foundation, and derive value from data assets. He has developed many innovative solutions enabling new business models and reimagination of business processes. In his previous role as head of Capital Markets Consulting and Solutions, he specialized in capital markets and risk management. He has led many front-to-back transformations and regulatory programs for leading Wall Street firms and has been involved in setting up new business functions in global banks.

TATA CONSULTANCY SERVICES

Awards and accolades

TOP 3 IT SERVICES BRAND

FASTEST GROWING IT SERVICES BRAND FOR THE DECADE 2010 - 2020

Contact

For more information on TCS' Banking, Financial Services, and Insurance (BFSI) unit,

visit https://www.tcs.com/banking-financial-services, https://www.tcs.com/capital-markets,

and https://www.tcs.com/insurance

Email: bfsi.marketing@tcs.com

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is a purpose-led transformation partner to many of the world's largest businesses. For more than 50 years, it has been collaborating with clients and communities to build a greater future through innovation and collective knowledge. TCS offers an integrated portfolio of cognitive powered business, technology, and engineering services and solutions. The company's 500,000 consultants in 46 countries help empower individuals, enterprises, and societies to build on belief.

Visit **www.tcs.com** and follow TCS news **@TCS**.

Corporate Marketing | Design Services | M | 01 | 22