Infosys topaz | AI in Financial Services

VIEW POINT

ACCELERATING AI IN RISK, COMPLIANCE, AND SECURITY MANAGEMENT

Infosys®
Navigate your next

A key goal of financial regulators is to provide banks guidelines for establishing adequate checks and controls to manage risk and protect the capital and interests of customers. However, over the past couple of decades, regulatory compliance has evolved from a mandate to an integral part of businesses. Banks are spending large amounts – both from a technology and business standpoint – on ongoing transformation of risk, compliance, and security functions. Technology intervention is driving efficiency in the management of various risks – credit, operational, market, financial, fraud, cybersecurity – on one side, and on the other, enabling compliance with current and emerging regulations. Many banks are assigning separate CXOs to oversee risk and compliance, and cybersecurity because of the growing challenge, complexity, and importance of managing these functions.

Gartner forecasts a 14% increase in security and risk management end user spending and it is anticipated to reach $215 billion in 2024.[1] While banks' security and compliance costs are increasing year-on-year (YoY), their risks are not mitigating at the same pace. AI can play a key role here by enhancing risk and compliance management efficiency in financial institutions.

AI everywhere

There are lots of established AI use cases in the risk, compliance, and security function that are helping to reduce fines, improve operational efficiency, and enhance customer experience. Some are listed below:

Anti-money laundering is one of the earliest use cases for AI; AI identifies anomalous and fraudulent transactions to save banks from paying enormous fines or incurring huge losses. Thanks to early identification of fraud and security risks, banks can take preemptive action against adverse events. Today, a proactive security stance is a priority because fraudsters are also turning AI-savvy, using neural networks to find loopholes, riding on social engineering to commit identity fraud, and injecting prompts to manipulate systems. Banks need AI to fight these AI.

AI expands the customer view, accessing internal and external data sources for insights into past behavior and transaction history, to enable banks to build a more accurate risk profile of every customer, and take better-informed credit decisions. Banks can similarly risk-profile every transaction at every touchpoint to decide if it is risky or not. Apart from providing more data, AI writes better scenarios and analytical models for predicting risk in all these cases.

With AI, banks can take better lending decisions (mitigate credit risk), forecast market trends, predict customer demands, keep pace with the changing spaces across markets, and understand the things they should or should not be doing from a regulatory and compliance perspective.

The customer, transaction, and operational risk management are part of the building blocks leading up to an overarching AI-based risk management framework that is helpful for calculating and managing banks' risk at an overall level. The framework is also useful for testing, and being prepared for, various stress scenarios as demanded by regulators.

Banks can mitigate operational risk and improve resilience by leveraging AI for process evaluation, predictive maintenance, and triggering timely alerts and decisions; in addition, they can improve operational efficiency by enhancing the performance of technology tools and platforms, and automating a number of manual processes and touch points. Many of our client banks are running AI pilots for managing (and continuously testing) operational risk controls; here, AI studies historical data patterns to predict which operational risks could create issues for the bank. In general, the use of AI has improved banks' ability to manage operational risk and resilience controls within the organization.

Like it has done in so many contexts, AI can capitalize on its rich insights to improve customer experience by reducing friction (for example, automated KYC), improving turnaround time (faster onboarding or loan disbursal), and enabling self-service and personalization.

However, when banks increase the use of AI for managing risk, compliance, and security, they also increase their exposure to AI-related risks. Apart from accentuated data-related risks – privacy, security, and confidentiality – there are challenges stemming from the AI models themselves, such as (a lack of) transparency and explainability, a point that is revisited later in this article.

From first in AI to AI-First

AI adoption in risk, compliance, and security is more advanced than in almost any other banking function; risk and compliance (AI) use cases are achieving faster and better results (than other use cases) to accelerate the transition to full-scale adoption. But first, banks need clarity on how to augment what they are doing; how to improve efficiencies with AI-based automation; and how to "mainstream" AI by using it in core risk identification and response functions.

An AI-First approach can help them with these issues

Simply put, AI-First means considering AI before other options for solving a problem. However, it is important to note that when it comes to risk and compliance the AI solution must necessarily be transparent and explicable; a "black box" will never pass regulatory scrutiny.

An AI-First approach brings the possibility of higher accuracy and efficiency, particularly through the use of the latest innovations, such as GPT. For example, banks are running PoCs to do unprecedented things, such as auto-resolve fraud by embedding GPT and automate control testing to ascertain how service agents treat customers (instead of manually listening to a random sample of agent-customer conversations). By bringing transparency to agent-customer interactions, banks can check for bias, incomplete disclosure, or any other regulatory violation in the service experience.

An important point is that even with an AI-First approach, banks must have a human in the loop to oversee the working of their AI models.

What next?

A progressive increase in AI usage and AI-related risk is inevitable. Going forward, financial institutions will need wider-reaching measures to stay on top of the increasing risk and the additional compliance mandates that will follow. Besides setting up governance frameworks and controls internally, banks should work with fintech companies to create better AI tools for risk and compliance. Last but not least, they should proactively engage with regulators to influence policymaking and demonstrate that they are trustworthy organizations working in the best interests of their customers.

References

[1] https://www.gartner.com/en/newsroom/press-releases/2023-09-28-gartner-forecasts-global-security-and-risk-management-spending-to-grow-14-percent-in-2024#:~:text=Worldwide%20end%2Duser%20spending%20on,estimated%20to%20reach%20%24188.1%20billion.

Authors

Amit Khullar
Global Portfolio Head - Banking, Risk & Compliance Domain Consulting
amit.khullar@infosys.com

Amit has 25+ years of experience in business consulting and large transformation initiatives. He has worked with global financial services organizations in regulatory and risk management programs and is leading AI-First vertical strategy for financial services.

Navdeep Gill
GRC Practice Lead- Financial Services
Navdeep_Gill@infosys.com

Navdeep leads the Governance, Risk, and Compliance (GRC) practice for the Financial Services vertical at Infosys. She is responsible for the overall go-to-market strategy, new service line, competency development, and delivery of all GRC programs, globally. Over her career, Navdeep has led multiple GRC transformational programs for leading financial institutions. She has wide global domain expertise and process competency across GRC, operational and enterprise risk, IAM, and financial risk management.

Anu Beri
Global Lead- RegTech Domain Consulting
Anu_Beri@infosys.com

Anu leads the RegTech segment globally for the FS Domain Consulting Group. Her portfolio includes Fin Crime compliance and Reg Reporting. Anu has a work experience of 25 years – working for global FIs out of India and London. Experienced in incubating and scaling capabilities for organizations and creating business solutions, she has in-depth knowledge of the various aspects of the FS industry, ranging from capital markets to wealth management to retail lending to Reg implementations (as a service, utility models).

For more information, contact askus@infosys.com

Infosys®
Navigate your next