International Journal of Multidisciplinary Research and Growth Evaluation.

Model Risk Governance for AI-Based Compliance Systems in Investment Banking

Pratik Chawande
Independent Researcher, USA

* Corresponding Author: **Pratik Chawande**

Article Info

ISSN (online): 2582-7138
Volume: 06
Issue: 03
May - June 2025
Received: 04-06-2025
Accepted: 05-07-2025
Page No: 2027-2035

Abstract
The emergence of artificial intelligence (AI) in the financial services sector, especially in investment banking, has drastically transformed the role of adherence. However, it also dangles unprecedented issues surrounding model risk governance (MRG). This paper assesses the impacts of the AI-based compliance systems management in the system of regulatory expectations and examines existing gaps in model validation practices. With the black-box nature of most machine learning (ML) models, more interest is raised about the lack of explainability, fairness, and accountability in these models, particularly with changing regulations such as Basel III and Dodd-Frank and U.S. regulatory reports, such as Y-14 and 2052a. The study can integrate regulatory compliance, AI governance, and operational risk through a multidisciplinary approach, thus building feasible tactics to enhance model risk governance. It includes the best validation practices, lifecycle management, and documentation. In this paper, we will seek to assist risk practitioners and compliance leaders in building more transparent, auditable, and regulation-compatible AI solutions.

DOI: https://doi.org/10.54660/.IJMRGE.2025.6.3.2027-2035

Keywords: Model Risk Governance, AI-Based Compliance Systems, Investment Banking

Introduction

The AI and ML boost is causing the financial industry to transform, particularly on the compliance and risk management front. Investment banks are using AI-supported systems to monitor transactions in real-time, as well as fraud detection, regulatory reporting, and anti-money laundering (AML). Although AI could increase the efficiency of operations, it introduces different types of model risk: data dependencies- / algorithmic opacity-risk, or decision unpredictability-risk. This has seen regulators increase oversight and insist on explaining AI systems' ability, fairness, and ethical integrity. Rules like the Basel III and the Dodd-Frank Act, formulated on the traditional risk approach, are applied to AI (Lamba & Kaur, 2023) [1]. Agencies like the Federal Reserve (Y-14 reports) and the Office of Financial Research 2052a liquidity filings must govern their models with extreme diligence, even AI ones. MRG should now consider the peculiarities of AI, which have nothing in common with the traditional quantitative models. This article examines the modification of expectations of model risk supervision in investment banks through AI-empowered compliance facilities. It examines the present validation disconnection and interpretability problems, and offers usable governance structures that align with real-life regulatory requirements.

The Rise of AI in Compliance Functions

Artificial Intelligence has now found its way into the operational structure of investment banking, especially in compliance. Due to the ever-growing regulatory oversight of financial institutions, the sheer quantity of structured and unstructured data these establishments have to process continuously and report has brought a revolution. Conventional compliance procedures, mainly based on manual work and a rule approach, have been found ineffective due to the complexity of global operations and changing regulatory requirements (Lamba & Kaur, 2023) [1]. To perform compliance-related functions and scale them, AI, primarily Machine Learning (ML), Natural Language Processing (NLP), and Robotic Process Automation (RPA) are being implemented now. The regulatory compulsion to identify and report wonder activities in real-time is one of the principal triggers of AIs or AI adoption (Paleti, 2022) [4]. The systems used to monitor transactions based on AI can scan thousands of transactions per second, detect an anomaly, and adapt dynamically to new risk trends. For example, deep learning is employed in detecting money laundering typologies based on previous SARs. These models can also change their interpretation with the arrival of new information, so they are much more effective than any static rule-based engines. AI also plays a vital role in regulatory technology (RegTech), facilitating document organization, contract intelligence, and regulatory change management (Paleti, 2024a) [2].

The regulatory documents, which are being parsed, with the help of NLP algorithms, include the Basel III Accord, Dodd-Frank Act, and Mifid II, and are mapped to internal policy documents and operational controls. Such ability not just accelerates the compliance lifecycle, but also eliminates human error in decoding and practice. The application of AI in the sphere of Know Your Customer (KYC) and client onboarding optimizes the work, automates document processing, recognizes the identity, and assesses the risk. Facial recognition with an AI-based background check allows banks to ascertain whether a new client is legitimate and how risky they are to work with quickly (Aziz & Andriansyah, 2023) [3]. Besides, sentiment analysis has started being located on customer communication channels, e.g., emails, chats, voice records, etc., to detect misconduct or insider trading alarms. Regardless of their breakthroughs, implementing AI in compliance is not free of issues. Such models are usually not transparent, which causes a significant concern to auditors, compliance officers, and regulators (Paleti, 2022) [4]. Advanced artificial intelligence, specifically, deep learning and ensemble models, is akin to the concept of the black box, rendering an explanation of the calculations behind certain risk levels or decisions unusually difficult. Such opacity predisposes to compliance risk by itself, at least when the laws come with explanation and traceability of models. Regulatively, the fast implementation of AI in compliance systems is beating governance policies that are not keeping pace. Regulators, including the U.S Federal Reserve, OCC, and the European Central Bank, have released guidelines promoting AI innovation and requesting well-implemented governance systems. The lack of a consistent regulatory approach to AI implementation further complicates the situation and is essential for worldwide operating institutions. There can be a patchwork of compliance with the definition of AI-related risk differing across jurisdictions.

Model Risk Governance: Traditional vs. AI Context

In financial terms, Model Risk Governance (MRG) can be defined as the entire set of practices deployed to control and address the risks arising from financial modeling. These practices in a conventional banking environment have come of age over decades; they are based on regulatory expectations like those in the U.S. Federal Reserve SR 11-7 and the OCC 2011-12. The customary type of model was a deterministic model, typically constructed via linear regression or time-series analysis, and assumptions that were easily outlined, tested, and could be recognized by the modeler and validators. These traditional models were fairly transparent, with specific mathematical correlations among inputs and outputs. In these terms, the model governance was targeted at appropriate data quality, testing the modeling assumptions, sensitivity to the input variation, back-testing the model performance against the real performance, and adequate documentation. When validation was carried out periodically, it was due to events. Usually, this was organized whenever models were being developed or there had been a material change in the business environment. In most situations, the separation of duties between designing the model, validating the model, and utilizing the model was well defined to prevent corruption of governance through subjectivity (Ogunmokun, Balogun, & Ogunsola, 2021). Conversely, AI and ML models incorporate a profound departure from these conventional arrangements. The models are frequently non-parametric and execute in high-dimensional feature spaces, so understanding how they work is opaque or complex. Deep neural networks, such as random forests or gradient boosting ensemble methods, and unsupervised learning have no conventional statistical interpretation. In turn, the traditional validation methods, such as the residual diagnostics or coefficient significance testing, are usually useless or inappropriate.

Explainability is one of the worst governance issues of AI models. In contrast to the traditional models, where the results may be traced back to the particular variables or assumptions, AI models are often a black box. This poses a significant challenge to internal risk management and regulatory compliance in general and in frameworks where regulators/senior management must be able to understand models, in particular. Methods including SHAP (SHapley Additive exPlanations) and LIME (Local Interpretable Model-agnostic Explanations) have also been suggested to fill that need. Still, these methods do not always work in all situations or to the same degree. Dynamic behavior is yet another critical issue. The older models are sometimes part of a static model; they do not evolve except when a re-calibration is done. However, AI models will be re-trained or self-adjusted in many cases, notably in adaptive learning systems or reinforcement learning applications. Such continuous change casts a significant doubt on version control, traceability, and how often the validation should occur.

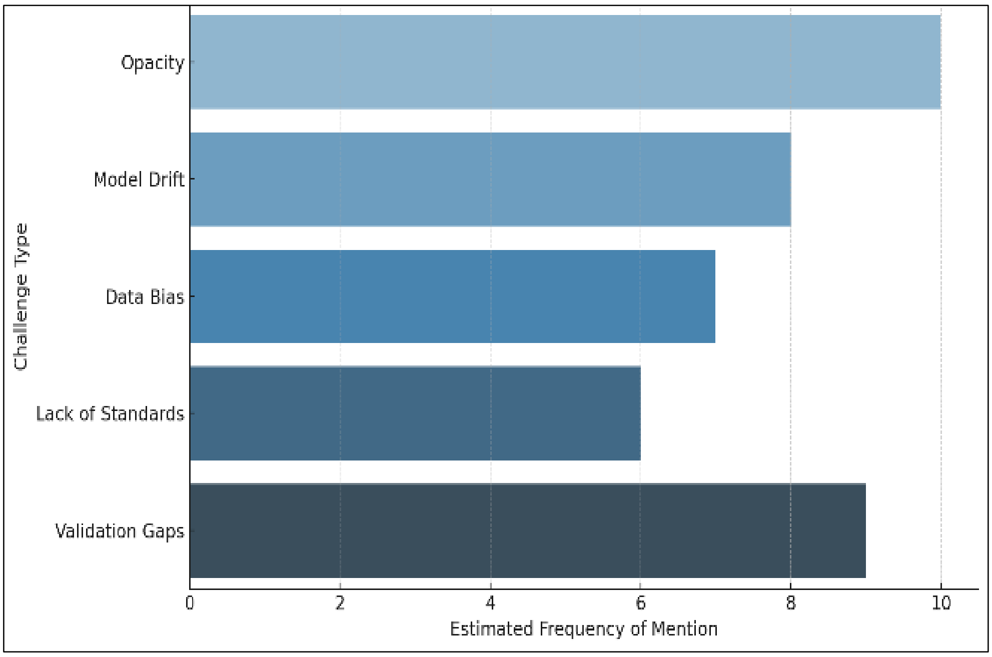


Fig 1: Governance Challenges in AI Model Risk Management

The model working well during deployment may act quite differently 6 months later, retrained on new data, and may not comply with the regulations or ethical principles. Besides, there is much greater data dependence on AI models. Training and testing of AI models need massive datasets. This risks the data quality, completeness, the labels' accuracy, and the data's representativeness. The model trained on incomplete or biased information can produce false or discriminatory output, which has real-life implications in such fields as AML monitoring or credit ratings. The generalization of such avoidance is that the data is already prescreened or audited, which fails in AI applications due to live data streams and third-party data use. Model lifecycle management is another issue of governance. The conventional models typically take a linear development and have clear stages, i.e., design, development, validation, implementation, monitoring, and retirement. Conversely, artificial intelligence models tend to have an iterative, non-linear progression. Progressive advancement, reskilling, and refinements make it challenging to identify the fixed checkpoints or milestones to verify (Paleti, 2024b) [5]. This dynamic requires the unceasing monitoring performance of models (MPM) that must be implemented into operational processes and accompanied by automation.

Regulatory-wise, the existing (legacy) compliance frameworks cannot keep abreast of this change. Although basic, SR 11-7 does not have AI as its design. It proposes a solid governing structure and stresses the necessity of model inventories, validation independence, and documentation, but specifics on attracting governing with opacity in models, adaptation to changes in real-time, and addressing ethical aspects peculiar to AI systems are not given in it. That is why most banks have to read available guides imaginatively, and they are also looking for new developments on a global scale, including the EU AI Act and suggested amendments in the Basel Committee on Banking Supervision.

Regulatory Expectations and Frameworks

With AI being rapidly implemented into financial services, especially in compliance and risk management areas, regulators worldwide are developing new guidelines to ensure that the technologies are used responsibly. Though some of these frameworks are still continuously developing, one of their key areas of interest is intransparency, accountability, data ethics, and operational resilience. In the context of investment banks, however, the rising requirements must be retrofitted into the current compliance architectures (based on traditional financial regulations) and fulfilled. SR 11-7 issued by the Federal Reserve and Bulletin 2011-12 of the OCC form the guiding principles on model risk management in the United States. These papers highlight the importance of model inventories, independent validation, performance monitoring, and efficient governance setups. Although these principles were not originally specified in the context of AI, their scope has now expanded to include more advanced types of ML. SR 11-7 is expected to give institutions the same treatment that statistical or econometric models should receive: AI-driven systems are to be treated as a model. The fundamental non-transparency and malleability of the AI systems make it challenging to use these established norms (Paleti, 2023) [6].

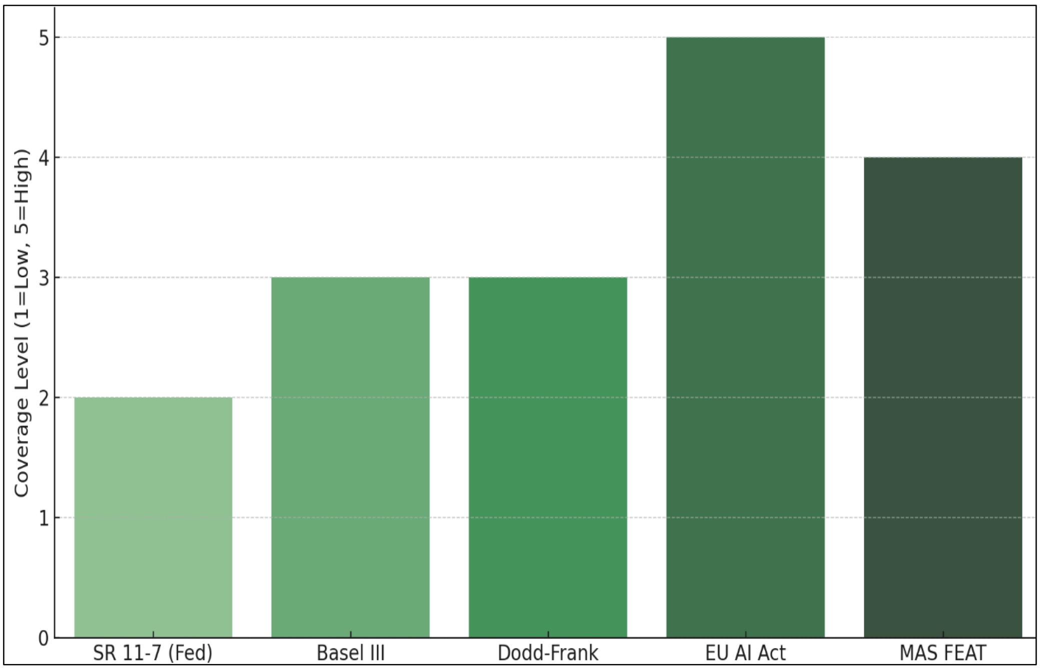


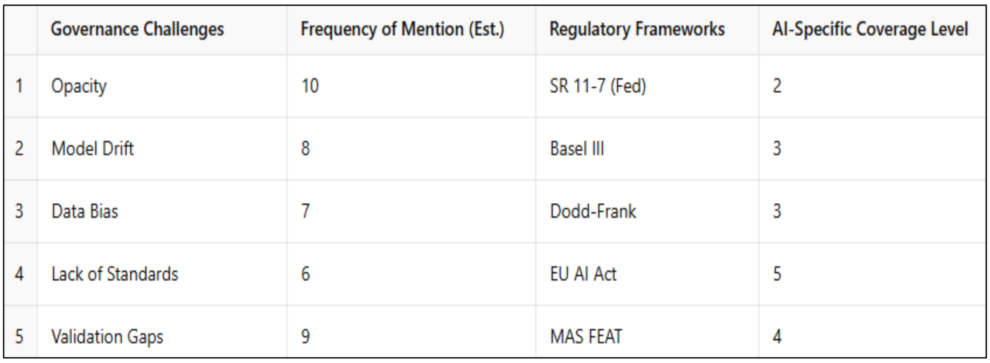
Fig 2: Regulatory Framework Coverage for AI Model Governance

The additional pressure is created by Basel III and Dodd-Frank Act regulation, which demands that banks show they support their capital and liquidity assessments with model risk sound judgment. With the Comprehensive Capital Analysis and Review (CCAR) and the Dodd-Frank Act Stress Tests (DFAST), the major financial institutions are required to demonstrate that their proprietary models, which are also based on AI, can forecast unfavorable scenarios with a significant improvement in accuracy under hypothetical stress conditions. Such training activities require a high level of model transparency and explainability--properties that do not come easily to most deep learning models. Consequently, to overcome the regulatory challenges, banks deploying AI in credit scoring, market risk modeling, or liquidity forecasting will be forced to comply with model interpretation frameworks, filter scenario analysis, and outline all the assumptions in a way expected to pass the regulatory examination. Two reports submitted by bank holding companies to the Federal Reserve, the Y-14 and 2052a reports, are used as important stress test supervisory tools and liquidity risk monitoring data. Any model used to generate such reports based on artificial intelligence has to be of utmost governance because data inaccuracy can hugely affect the macroprudential evaluation (Ogunmokun, Balogun, & Ogunsola, 2021). The regulatory feedback has also stressed additional points that the output of AI-based models underlying such reports should be explanatory as well as reproducible. It is also promoted that institutions ascribe trace logs and audit trails depicting each version, re-training event, and decision point in the model's lifecycle. Crossing the U.S border, international regulators are also making courageous steps toward dealing with AI in finance. However, the most substantial is the AI Act introduced by the European Union in 2021. It defines the AI systems utilized in the financial services, including those detecting creditworthiness, helping detect fraud, and monitoring compliance, as high-risk. These systems are under the harsh requirements of data governance, transparency, human control, and strength.

Through the Act, companies must perform a rigorous conformity evaluation, report to regulators, and enable end users to interpret AI-driven decisions and challenge them. Non-compliance may imply fines of up to 6 per cent of the turnover per annum in the world. FCA UK and the Bank of England also published joint discussion papers spelling out how they expect AI to be governed. They are principles-based; they emphasize proportionality, transparency, and accountability (Aziz & Andriansyah, 2023) [3]. The FCA underlines that financial institutions should properly control AI systems that provide fair results to consumers and comply with current rules of conduct and prudence. With the help of their sandbox programs, companies can also test AI models in a regulated environment with regulatory oversight, which is becoming increasingly popular in multiple jurisdictions. Meanwhile, regulators in the Asia-Pacific region, i.e., the Monetary Authority of Singapore (MAS), the Hong Kong Monetary Authority (HKMA), and the Japan Financial Services Agency (JFSA), are introducing soft regulations, advisory frameworks, and industry coordination to encourage responsible AI. The FEAT by the MAS (Fairness, Ethics, Accountability, and Transparency) are clear and unambiguous principles of the governance of AI in the financial services. The concepts encourage institutions to demonstrate the validity of training data, explain essential decisions, and develop escalation channels for AI choices that influence clients considerably.

Gaps in AI Model Validation Practices

Due to the massive scale at which AI systems are gaining recognition in the financial sphere, especially in the compliance and risk management sectors, it has become a serious issue that the current model validation processes are incapable of covering the unique factors and paradigm of AI/ML models. Model validation was already an established part of an organization in financial institutions, where traditionally their scale has been pegged on quantitative risk models such as Value at Risk (VaR) or credit scoring. The move to AI has revealed a deep flaw in the methodology and thinking. These failures lead to severe regulatory, reputational, and business risks, particularly when AI models are deployed in high-stakes systems, like anti-money laundering (AML), regulatory reporting, or transaction surveillance.



	Governance Challenges	Frequency of Mention (Est.)	Regulatory Frameworks	AI-Specific Coverage Level
1	Opacity	10	SR 11-7 (Fed)	2
2	Model Drift	8	Basel III	3
3	Data Bias	7	Dodd-Frank	3
4	Lack of Standards	6	EU AI Act	5
5	Validation Gaps	9	MAS FEAT	4

Fig 3:

Interpretability is one of the most significant gaps among them, in contrast to the typical model where the inputs and their mathematical connection are exposed and checkable, AI models, notably deep learning and ensemble methods, are black-box, high-dimensional systems. Post-hoc explanations. Such tools as SHAP and LIME only give approximate post-hoc explanations. However, they are soon unintuitive when supplied to validators (not usually technological), risk committees, or regulators. Practically, a significant number of validators do not have the technical expertise to evaluate the behavior of AI models effectively, and considering this fact, such an overview might be shallow and fall short of questioning the design and assumptions behind the models, as well as testing fairness, bias, or drift. The second essential problem is the absence of standardized validation frameworks in terms of AI. Most financial institutions use risk validation manuals based on SR 11-7-era advice focusing on stability, backtesting, and performance metrics such as RMSE, AUC, or Gini coefficients. These are still critical but do not suffice to support AI systems with a nonlinear nature, non-stationary properties, and sensitivity to unbalanced or incomplete data. For example, conventional metrics suggest superior performance but do not detect subgroup bias, susceptibility to attack, or overfitting to artificial/past trends. Data quality and lineage validation are other areas that have not been addressed sufficiently. AI machines have an appetite and instead consume diverse and dynamic data, such as social media, third-party vendors, and real-time flow of transactions.

Model Validation

A crucial step in model validation that is often underestimated is ensuring training and validation datasets are representative, de-biased, and complete. The data validation of the data has been treated as a distinct role in many firms and seen as an orphan with little connectivity to the model risk processes. It creates information gaps in understanding how data anomalies or hidden biases affect model behavior and subsequent compliance models. Further, the conventional validation methods are based on a single, stationary evaluation implemented before model implementation. Nevertheless, AI models, specifically those in production, keep learning, adapting, or drifting over time (Singireddy *et al*., 2021) [10]. This is called model drift due to shifts in the hybrid data distribution, user behaviour, or market conditions. Models are subject to weak ongoing validation and performance check systems, gradually losing quality. They may pose these risks that are not apparent until regulatory inspections or the collapse of their systems. Most institutions have no automated system of monitoring or early warning signs that can be used to monitor drift in real time.

Practical Governance Strategies for AI Model Risk

As AI and Machine Learning (ML) technologies become integral to compliance functions in investment banks, robust Model Risk Governance (MRG) becomes essential to address challenges such as opacity, data dependency, and adaptability. Financial institutions must implement effective strategies to manage these risks and align with regulatory standards. Below are key governance strategies for AI model risk:

1. Frameworks of specific ai validation

AI-specific validation frameworks are necessary to address the unique characteristics of AI models, such as their black-box nature. Like linear regression testing, traditional validation techniques are ineffective for AI models. Key components of AI validation include:

- **Bias Testing**: AI models are sensitive to the data they are trained on. Bias testing ensures the model does not disproportionately impact specific groups (Singireddy *et al*., 2021) [10].
- **Explainability Assessments**: AI models must be interpretable. Tools like SHAP (SHapley Additive exPlanations) and LIME (Local Interpretable Model-agnostic Explanations) can help generate transparent outputs (Lamba & Kaur, 2023) [1].
- **Hyperparameter Documentation**: Documenting hyperparameters ensures transparency and proper tuning of the AI models (Paleti, 2024a) [2].

Table 1: Examples of Specific AI Validation Techniques

Technique	Purpose	Example
Bias Testing	Detect and mitigate bias in model predictions	Fairness testing in credit scoring models
Explainability Assessment	Provide transparent and interpretable model outputs	SHAP, LIME for model explainability
Hyperparameter Documentation	Track and manage model configuration settings	Documenting hyperparameter optimization steps

2. Inventory Control Model

Maintaining a comprehensive AI model inventory is crucial. This inventory should include details on model inputs, assumptions, training data sources, and validation cycles. By maintaining transparency, organizations ensure their models are traceable and regulatory-compliant (Paleti, 2023) [6]. This inventory also facilitates regular reviews and performance monitoring to manage the risks of rapidly evolving AI systems (Sayles, 2024) [9].

Table 2: Key Elements of AI Model Inventory

Element	Description
Model Inputs	Data and features used for model training
Assumptions	Theoretical or operational assumptions in the model
Training Data Sources	Origin of data used for training (internal, external, public datasets)
Validation Cycles	Frequency and criteria for model validation

3. Incessant Surveillance And Re-Training

Continuous surveillance is essential to detect model drift, where performance degrades over time due to shifts in data. Implementing real-time monitoring systems and automated re-training mechanisms ensures that models remain effective (Singireddy *et al.*, 2021) [10]. Automated alerts can notify risk managers of significant changes in model performance, prompting timely re-validation.

Table 3: Example of Continuous Surveillance and Re-Training Process

Process	Description
Real-Time Performance Monitoring	Track model performance metrics (accuracy, precision, recall)
Drift Detection	Identify shifts in data distribution.
Automated Re-Training	Trigger re-training when performance thresholds are breached.

4. Oversight Human-In-The-Loop

Despite advances in AI, human oversight is crucial for ensuring compliance. Human-in-the-loop (HITL) systems involve embedding human validation at decision points where AI impacts customer compliance. This ensures that AI models do not make erroneous or biased decisions. Compliance officers or legal teams should validate critical AI decisions per regulations like Dodd-Frank and SR 11-7 (Ogunmokun, Balogun, & Ogunsola, 2021).

Table 4: Human-in-the-Loop Oversight Process

Step	Description
Decision Review	Compliance officers review AI-driven decisions.
Validation of Critical Outputs	The legal team validates outputs with potential consequences.
Final Approval	Human approval is required before a final decision or action.

Implementing AI in compliance systems presents governance challenges, particularly transparency and adaptability. To mitigate these risks, investment banks must adopt AI-specific validation frameworks, maintain model inventories, implement continuous surveillance, and ensure human oversight at key decision points (Singireddy *et al.*, 2021) [10]. These strategies will ensure that AI models are transparent, compliant, and ethically sound.

Real-World Implementation: Insights from Regulatory Experience

It is not a concept anymore but a reality that the application of AI-based compliance in investment banking is currently reshaping regulatory processes in most parts of the world. Nonetheless, many operational, governance, and organizational challenges stand between a conceptual model and a production-ready, regulatory-compliant deployment. Based on the practical experiences of financial organizations operating within the regulations of such systems as the Basel III, the Dodd-Frank Act, federal laws, and others (Y-14, 2052a), it is clear that the implementation of AI can be used to optimize compliance, but only with a fully developed governance structure that is cross-dimensional. Another of the most frequent lessons is that regulatory alignment has to start with the design phase of the AI model lifecycle, but not after it. As an illustration, in the case of institutions that are subject to Comprehensive Capital Analysis and Review (CCAR) and DFAST stress tests, the AI models aimed to assist in measuring credit or liquidity risks need to be directly linked to the regulatory definitions of loss, exposure at default, or liquidity coverage ratio (LCR). Unless this alignment is guaranteed at the beginning, the model outputs can be deemed non-compliant, resulting in last-minute overrides or supervisory refutals (Vettriselvan *et al.*, 2025) [8]. At a few leading investment banks, internal design of AI models now starts with what is known internally as regulatory use case mapping: a system in which every potential output of AI is brought to bear on every potential regulatory filing line item, policy clause, or control functionality. For example, the AI model, which predicts the probability of a suspicious transaction, should be an inarguable feed to processes that fall under the Bank Secrecy Act (BSA) and Fincen reporting guidelines. Organisations such as distributors are starting to implement organised taxonomies and metadata registers to monitor and authenticate.

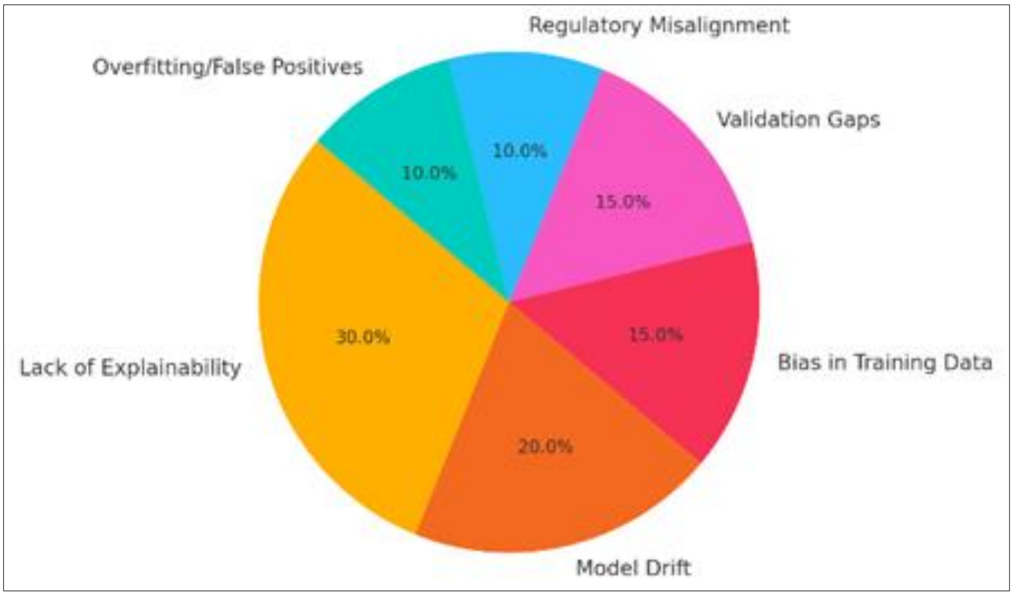


Fig 4: AI Risk Categories in Investment Banking Compliance

Among some of the more recognizable implementation strategies that are becoming more widely used, there is a practice to rely upon so-called AI Model Sandboxes that are risk-contained, closed environments where models are to be tested against historical compliance incidents, stress scenarios, and false positive/negative ratios before any deployment. Such sandboxes are supervised by independent model risk units and audit teams that are objective. As it is, it will enable institutions to calibrate AI model sensitivity without putting themselves at either an operational or reputational risk (Sayles, 2024) [9]. In the case of AML, banks have used sandboxes to test how the models behave on known money laundering networks, where they have known criminals who can test the models and find potential blind spots or weaknesses in pattern recognition. The practice in the real world has also indicated that human-in-the-loop oversight should be embedded, particularly on AI systems that involve decision-making. Supervisory agencies regularly emphasize the necessity of responsible human beings to monitor significant results related to compliance. Consequently, tiered escalation mechanisms are being implemented by institutions, where particularly significant or ambiguous model decisions, e.g., decisions not to accept a customer onboarding application or characterize a trade as insider-driven, are decided by compliance analysts, counsel, and legal advisors, prior to absoluteness. This not only meets the requirements of the regulation in the SR 11-7 and OCC 2011-12, but also contributes to getting rid of the decisions that are not sensible or are biased. In addition, teamwork between compliance, risk, audit, and data science teams has proved key to implementation. In most companies, the compliance officers were not tech-savvy regarding AI, and the data scientists were not conversant with the laws. The banks have resolved to fill this gap by establishing cross-functional artificial intelligence governance committees, where all the stakeholders in the involved departments are convened to develop and inspect the models collectively. This collaboration mechanism encourages collective responsibility, compliance with the regulatory expectations, and accelerated and safe innovation (Paleti, 2023) [6]. Other organizations have also implemented in-house AI literacy training to increase the capability of non-technical employees. In the case of line-of-business employees who use AI tools daily, they know their capabilities and constraints.

Another field in which implementation can be improved is documentation discipline. Due to feedback gained by regulators, particularly in the Dodd-Frank and Basel III supervisory checks, the institutions have resorted to using well-structured and version-controlled

Documentation processes. All the models come up with traceable metadata on data source, training iterations, performance indicator, factors based on which retraining is to be initiated, ethical reviews, and approval points. Large portions of this process have been automated with the utilization of AI lifecycle management tools, which can be built to cloud providers such as AWS SageMaker or Azure ML Studio. These tools create logs and dashboards that allow internal auditors and regulators to obtain real-time snapshots of model performance.

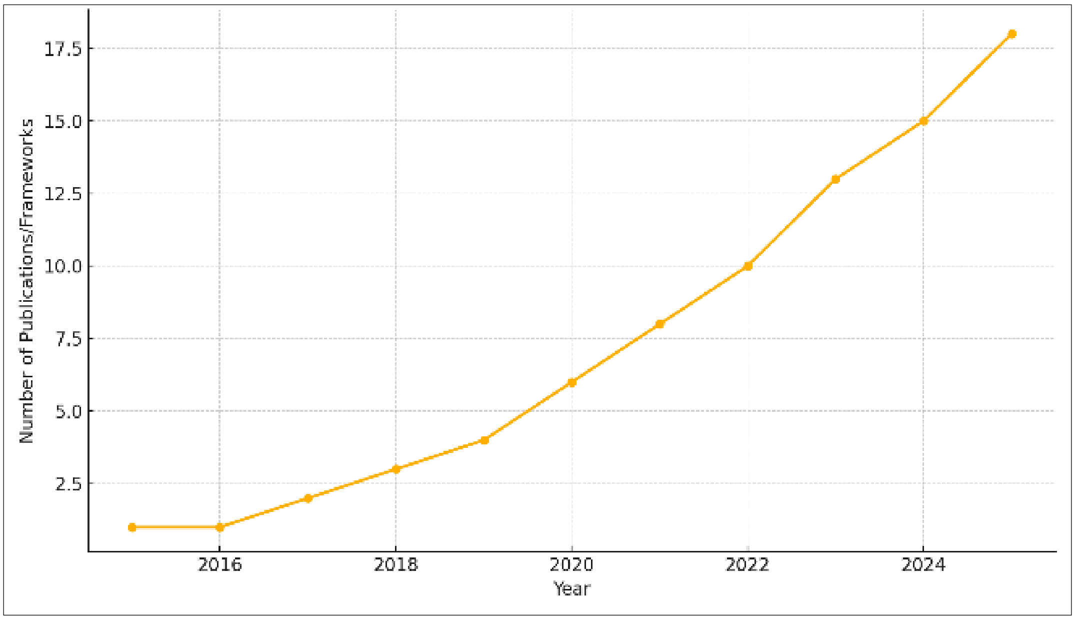


Fig 6: Growth in Regulatory Publications on AI Risk Governance (2015-2025)

In systems terms, the deployment of AI models in production is becoming more and more linked, in the context of AI models, to model performance monitoring (MPM) dashboards, which will be glued to control rooms and compliance reporting engines. These dashboards monitor accuracy, drift, change in feature contributions, and the volume of predictions within various business segments or geographies (Sayles, 2024) [9]. Notably, they also monitor the level of the so-called alert override, i.e., when AI results are overruled by human compliance staff. Poorly performing models or knowledge gaps in contexts and high override rates might indicate that the model needs to be retrained or recalibrated.

Regulatory harmonization in the local context is a difficult challenge in prominent international organizations, particularly when AI systems are deployed across different jurisdictions. A model trained in the United States data and regulatory environment may fall short of the European GDPR Standard or the data residency laws of the APAC region. Companies have started localizing AI models, adapting parameters, sets of features, and governance mechanisms to deal with jurisdiction legislation. They also explore so-called model variant inventories to trace the models operating in which regions, under which assumptions, and within which degrees of control. The implementation strategy has also been affected by honest feedback from the regulators. For example, third and fourth parties have questioned the importance of explainability and reproducibility of complex AI-driven models in forecasting liquidity under 2052a reporting to the U.S. regulators (Singireddy *et al*., 2021) [10]. As a reaction, some banks have started implementing dual model systems, one of which they can explain to regulators (regulatory model) and the other, a second and more advanced model based on AI (strategic model). The interpretable model typically applies generalized linear models (GLMs) or decision trees, which parallel those produced by AI without being cryptic enough to allow compliance obligations, yet still being transparent and explanatory to humans.

Conclusion

Implementing Artificial Intelligence in compliance systems symbolizes a seminal transition in the approach toward managing the risks of investment banks, on-demand by regulatory bodies, and keeping operations efficient. Nonetheless, this revolution also ushers in new challenges in governance, especially the model risk. Unlike traditional models, AI systems are dynamic, adaptive, and opaque, a characteristic that bothers conventional validation and oversight frameworks based on transparency and predictability. This paper has discussed the evolving governance of model risks of AI in the compliance functions, the challenges in the current validation practice, the regulatory expectations, and suggestions on the practical approaches to the governance. A thorough assessment of the frameworks used, including Basel III, Dodd-Frank Act, and critical regulatory submissions, including Y-14 and 2052a, illustrates that the supervising agencies are increasing the AI-based models' explanatory factors, fairness, and accountability. The need to integrate the viewpoint of the European Union (EU AI Act), United Kingdom (FCA principles), and the Asia-Pacific (regulatory trends) increases the necessity of a consistent and cross-jurisdictional approach to governance. There are also practical examples of global financial institutions implementing such systems fully that demonstrate that the successful deployment of AI-based Compliance systems depends on something other than the technical capacity of such systems. It necessitates cross-functional cooperation, investment in explainable AI efforts, resilient data governance, human-in-a-loop control, and lifecycle monitoring. Governance should also be transformed so that AI models are technologically sound, ethically responsible, operationally resilient, and legally compliant. Besides, cultural change is also vital. The organizations must develop a system: the complaint officers, risk managers, data scientists, and auditors should collaborate. Introducing more AI-related knowledge to teams, being transparent throughout all phases of model development, and securing ethical considerations within the AI lifecycle have ceased being optional initiatives; they are strategic necessities.

Disclaimer:

The views expressed in this work are those of the author and do not necessarily reflect the views of any current or former employers**.**

References

1. Lamba SS, Kaur N. Designing AI for Investment Banking Risk Management: A Review, Evaluation, and Strategy. In: International Conference on Emerging Trends in Expert Applications & Security. Singapore: Springer Nature Singapore; 2023. p. 329–47.
2. Paleti S. Data Engineering for AI-Powered Compliance: A New Paradigm in Banking Risk Management. Eur Adv J Sci Eng. 2024a;2(1).
3. Aziz LAR, Andriansyah Y. Artificial intelligence's role in modern banking: exploring AI-driven approaches for enhanced fraud prevention, risk management, and regulatory compliance. Rev Contemp Bus Anal. 2023;6(1):110–32.
4. Paleti S. The Role of Artificial Intelligence in Strengthening Risk Compliance and Driving Financial Innovation in Banking [Internet]. 2022. Available from: https://ssrn.com/abstract=5250770
5. Paleti S. Neural Compliance: Designing AI-Driven Risk Protocols for Real-Time Governance in Digital Banking Systems [Internet]. 2024b. Available from: https://ssrn.com/abstract=5233099
6. Paleti S. AI-Driven Innovations in Banking: Enhancing Risk Compliance through Advanced Data Engineering [Internet]. 2023. Available from: https://ssrn.com/abstract=5244840
7. Ogunmokun AS, Balogun ED, Ogunsola KO. A Conceptual Framework for AI-Driven Financial Risk Management and Corporate Governance Optimization. Int J Multidiscip Res Growth Eval. 2021;2.
8. Vettriselvan R, Velmurugan PR, Regins JC, Maheswari SU, Joyce R. Best Practices, Ethical Challenges, and Regulatory Frameworks for AI Integration in Banking: Navigating the Future. In: Artificial Intelligence for Cloud-Native Software Engineering. IGI Global; 2025. p. 377–410.
9. Sayles J. The Current State of AI Governance and Model Risk Management. In: Principles of AI Governance and Model Risk Management: Master the Techniques for Ethical and Transparent AI Systems. Berkeley, CA: Apress; 2024. p. 1–18.
10. Singireddy J, Dodda A, Burugulla JKR, Paleti S, Challa K. Innovative Financial Technologies: Strengthening Compliance, Secure Transactions, and Intelligent Advisory Systems Through AI-Driven Automation and Scalable Data Architectures. J Finance Econ. 2021;1(1):123–43.