Deep Science Publishing
https://doi.org/10.70593/978-93-49910-91-1_7

Chapter 7: Enhancing risk and compliance monitoring systems with artificial intelligence to achieve regulatory transparency and accuracy

7.1. Introduction

In line with principles espoused by financial services regulators across the globe, national or international supervisory or regulatory bodies will need to promulgate AI governance frameworks applicable to supervised financial institutions. Within financial services, the development of AI model governance is equally nascent and urgently needed. To support deployment of AI by financial services firms, guidance needs to be offered on the design and operation of effective AI model governance frameworks. This text attempts to set the stage for future collaboration between researchers and the practitioners. It ultimately proposes two orthogonal paths, aimed at garnering insights from adjacent domains and building solutions that would leverage regulatory technologies and related, cutting-edge tooling. In terms of domain cross-fertilization, solutions in adjacent domains with more robust AI governance, such as healthcare and autonomous vehicles, will need to be studied for applicability to financial services. Solutions developed in the financial domain with compliance oversight view would also benefit other industries with large and robust AI model frameworks in development (Anderson, 2025; Becker & Sharma, 2025; Brandt, 2025).

Within either path, a flexible and modular implementation supporting extensibility and easy adaptation of regimes to regulatory change should be expounded upon. Such a system provides a join-up with a systematic framework to conduct regulatory output assessments of AI models before and after they are deployed, and to proactively monitor and act on regulatory divergences thereafter. The capability to parse and interpret complex sets of rules and cases will refine engagement with AI model documentation and explication thereof, while offering a mechanism to automate compliance testing and aggregate and organize adherence results on location/usage basis. Such proactive compliance can be applied to retain business as usual oversight assurances and to request additional evidence as necessary. Furthermore, the appropriate governance structure and partnering strategy for achieved confidence in the above and offloading as necessary will be addressed (Chen & Lopez, 2025; Desai, 2025).

Fig 7.1: Enhancing Risk and Compliance Monitoring Systems

The capabilities envisioned may include a modular approach permitting the AI governance system to be tuned and adapted easily to various institutions and regions. Initially, rules of AI usage will need to be inputted into the system. Natural language processing and other AI methods may be employed to catalogue and parse these rules for systematic use in the governance solution. In the face of regulatory divergence, the active construction of new local rules from the central canon may be helpful, or adaptation to new models of an AI deterministically- or probabilistically-inferred from local models. Expanding rules as necessary through general AI systems trained on such diverse corpora is another option that likely could bear fruit. Approaches of this nature may aid in governance by assimilating substantially more rules than a human team typically would be able to process.

7.2. Understanding Risk and Compliance Monitoring

In 2021, a bank developed a fraud monitoring system that monitored transactions in real time to reduce losses from fraud. While stating that the monitoring system would be developed and deployed, it was later found that it had been replaced by an Excel-based manual process. This had resulted in huge financial losses over the years because the organization was not able to scale up fraud detection as per business changes or emerging methods adopted by fraudsters. At the time of this incident, regulations and policies governing fraud monitoring systems had already been in place for nearly a year. Risk and compliance monitoring systems typically require the tracking of various metrics, including system performance, data drift, model changes, input changes, and segmentation changes. Most of these metrics are well-defined, with elastic thresholds that can be established based on business history and model performance. The financial services and healthcare sectors have implemented a range of monitoring systems to enhance existing implementations. While computing and reporting of metrics may be scattered across systems, it is easier to correct mistakes in monitoring and reporting systems than in core risk and compliance systems.

Monitoring of AI/ML models is just as important as other regulatory tools such as performance reporting or policy setting. Existing monitoring systems used by banks often overlook key decisions taken before the deployment of the model. Banks with a large installed base of risk and compliance monitoring systems situations similar to the fraud monitoring system need to put a monitoring overhaul that complements existing implementations. It is extremely important to quantify risks in the algorithms used by AI/ML models to ensure the longevity of investments in AI and ML. Client attrition models that drive millions of dollars of income every year can lose a significant portion of that income overnight if there is a change in how dimensions are generated. In such an eventuality, it is generally too late to set an action plan and correct the errors.

7.3. The Role of AI in Risk Management

Current issues in model governance are examined, including gaps in FMiG, organizational model governance approach and model risk management challenges. The state-of-the-art compliance measures are presented under three main categories: the AI governance framework in response to regulatory requirements, governance process and responsibility monitoring tools such as model catalogues, review logs and compliance audit systems, and model risk management measures covering the risk assessment, testing and validation of models.

The wide range of application areas of AI systems ranged from simple areas like customer service, to more complex areas such as customer default prediction and loan assessment. AI systems additionally find use in critical aspects like operations risk and cyber fraud detection, which require high scrutiny and governance scrutiny. The involvement of advanced AI systems in broader and increasingly critical decisions has escalated an urgent need for compliance and effective model governance. Current model governance practices have evolved from traditional financial applications, and those practices are adapted from mathematical modeling and traditional financial governance frameworks. AI model governance currently involves complex review flows in the organization structure combined with manual review stamps on model documentation. However, as the unprecedented rate of growth of AI model complexity and architecture, concerns on current practices and sustainability arise.

The goal is to find the balance between regulatory requirements and internal governance requirements during rapid model development, and to maintain governance and compliance of the models during further deployment and enhancement. In particular, current challenges of AI model governance in the financial services industry are identified, including missing applications of best practices identified in the task force, gaps in the organizational model governance approach, and missing model risk management practices during preservation, monitoring, and compliance measures. In addition, a literature review is provided on the current state of the art compliance measures for both industry applications and academic approaches. The current compliance measures are categorized under three main categories, including the AI governance framework in response to regulatory requirements, governance process and responsibility monitoring tools such as model catalogues, review logs and compliance audit systems, and model risk management measures covering the risk assessment, testing and validation of models.

7.3.1. AI Techniques in Risk Assessment

Financial services firms are looking at ways to monitor automated, self-learning model behavior. Once a risk identification model is live, there is a need to monitor for data leaks, input drift, population drift, etc., and to monitor that the model is behaving as expected. This is a complex system that needs a robust monitoring framework. Risk models are sometimes against sensitive grounds like credit/loans. There is a strong need to monitor fairness metric bands to ensure that these models are not biased and the majority of the right data is being selected for the purpose intended. In both these systems, manual data monitoring and observability tools often require dedicated staff to monitor these systems promptly. Error investigation often takes a backseat quality concern, bringing about potential losses.

The data sets are huge in terms of records and fields. This volume of data is often in the form of large matrix structures. Many AI techniques, especially linear algebra-based ones, cannot work with such high-dimensional inputs. As a result, blueprints for observable features become a manual task. There needs to be more screening of generic observability features across types of data assets that will help protect the integrity of automated systems. The aim is to first monitor for a combination of statistical distribution-based data drift and geometric transformations. Then, it will send a batch of the top misses to an explainable AI model to generate actionable insight to determine whether data checks need manual investigations.

7.3.2. Machine Learning for Predictive Analysis

ML is one of the most crucial advancements of AI and symbolizes computing's ability to recognize patterns. ML has given rise to a plethora of new solutions inconsistently adopted across the global financial services span. These span diverse areas, such as service delivery, regulation, and fraud prevention, notably affecting operational resilience and operational risk. This abuse opportunity is paralleled by serious considerations regarding risks posed by the technology, notably around customer protection. Regulators have responded with rapid-fire policy and guidance issuance interspersed with more flexible principles-based approaches. Surveys cite AI's fitful ponderousness on the demand-side resulting from internal as well as external considerations: customer data, market dominance by some actors capacity to interpret outputs, as well concern over regulatory or reputational risks driven by many aforementioned considerations.

Underappreciated, wider system-level challenges here inter alia limit authorities' capacity to regulate. Hence, promising pathways exist in self-regulating data-driven AI to circumvent heavy-handed attempts to micromanage rapidly evolving systems. AI operated decision-making at scale is fast-approaching, interspaced with misalignment, harm, and critical incidents. Regulatory vacuum exists that necessitates regulated firms to tackle this coevolution challenge. Firms and authorities must regulate AI guiding its design and engineering. Plunging itself into a regulator's approval system prevents AI from competing and meeting stakeholders' needs. Inadvertently, resolution requirements hollow out AI advantages. Approaches differentiating stepping into quirks and frictions of AI decision-making with qualitative principles can prove effective. AI re-purposing of misused, misaligned data or feedback loop pre-appropriating ownership befit qualitative contingency constraints. The space of encoded advice structures: one predominant advice structure needs to be represented in separate but coherent ways and hierarchically-defined agent systems traversing no advice generation space need to be designed. Agents combat frictions from differing feedback domains, actions, condition, and modes, and agents harmonize with open engagement forcing discrepancy balancing moderation on risk adaptive shielding of conditional equality enforcement may be effective.

7.4. Regulatory Frameworks and Compliance Requirements

Compliance and risk management of the regulation framework and the compliance requirements should inherit the structural framework of the current risks control decomposition. Title effects are also critical to compliance based on the evolutionary models. The compositionality of risk and compliance entails a hierarchical decomposition approach, in which regulatory and compliance requirements and risk measurement models, tools, and mechanisms with compliance audits and breach reaction can be encapsulated in a hierarchical fashion, similar to layered architectures in networking and distributed systems. With this as the starting point, high-level regulatory frameworks and regulations can be refined into a tree structure of compliance requirements at compliance institutions with corresponding risk models and measurements. Multi-level compliance modeling is built accordingly, which entail a large diversity of compliance requirements for modeling.

Fig 7.2: Regulatory Frameworks and Compliance Requirements

For example, compliance and risk management for the European banking regulation framework can be done by examining the regulatory requirement of Basel III and its compliance requirements. In this example, the effects of regulations on banking institutions can be modeled in terms of the minimum regulatory capital requirements and capital buffer requirements based on the risk of bank assets hedged by modeled portfolios. The methods of compliance measurement can be implemented by examining the flow of cash into bank earnings with modeling. The effects of compliance breaches or audits can be accomplished by simulating gradual risk grades deterioration by the stress testing financial networks based on bank exposures. Then, equity short selling modeling can be realized with the agent-based market modeling of the asset selling agents. Compliance with the duration risk limit requirements with compliance defect mechanisms can also be examined by the modeling scheme designed.

7.4.1. Overview of Key Regulations

Financial services regulators are implementing new rules and regulations intended to lessen bias and misuse and enhance protection for consumers who use AI-enabled financial products and services. While many measures governing the use of AI are new or under consideration, several laws and rules are on the books in one form or another and are the starting point for compliance frameworks. The list of financial services regulations considered could differ by industry or even by financial services operating region. With that in mind, some key regulations are considered.

The Federal Fair Lending Laws aim to limit discrimination in consumer lending and promote fair and responsible lending. There are two primary acts: The Equal Credit Opportunity Act prohibits discrimination in credit transactions for factors such as race, sex, and marital status. The Fair Housing Act also prohibits discrimination in real estate transactions for similar classes of individuals, including familial status and disability.

The Dodd-Frank Wall Street Reform and Consumer Protection Act established the Consumer Financial Protection Bureau to implement and enforce federal consumer financial regulations, and, among other things, granted the Bureau authority to issue rules and regulations to prohibit unfair, deceptive, and abusive acts or practices. The Rule on the Collection of Consumer Debts prohibits debt collectors from a variety of practices intended to deceive consumers into forfeiting their rights. The Military Lending Act prohibits lending practices that could unfairly target servicemembers and their families by charging excessive fees.

The privacy regulations applicable to financial institutions, which include banks, credit unions, credit card companies, securities firms, insurance companies, or other companies engaged in certain financial activities, were enacted to protect personal information disclosed to these institutions, including names, addresses, social security numbers, account numbers, balances, and transaction histories. The Gramm-Leach-Bliley Act grants consumers the right to opt-out of information sharing, mandates the protection of sensitive information by financial institutions, and requires information sharing among businesses in the event of a merger, consolidation, or transfer. Violations can incur damages, attorney’s fees, and class action lawsuits. Companies must regularly review their privacy compliance programs and policies, and counsel should be involved in the design of policies, contracts, and disclosures regarding privacy.

7.4.2. Compliance Challenges in Financial Services

AI systems have found a wide range of application areas in financial services including credit scoring, event detection, fraud detection, money laundering detection, and trade execution. Their involvement in decisions has escalated the need and demands for compliance and effective model governance. In finance, current governance practices often struggle with the fundamental differences in characteristics between conventional and AI models. Examples of the differences include uncertainty in model assumptions vs. reliance on a predetermined distribution about the chances of something happening, and complicated mathematics such as partial differential equations vs. largely mathematical-free empirical patterns and interpretations. AI model governance frequently involves complex review flows and compliance queries to many parties. In addition, it also relies heavily on manual steps producing various documents, communicating with compliance / governance parties over emails, and obtaining manual sign-offs and decisions. As a result, AI model governance faces challenges in terms of effectiveness, cost, complexity, and speed. This paper focuses on the challenges of AI model governance in the financial services industry and highlights the importance and opportunities of adopting automation technologies. The goal is to realize a system-level framework towards increased self-regulating over robustness and compliance so that the review, monitoring, management, and mitigation capabilities are all integrated together with AI technologies. Such an approach helps to enable potential solution opportunities through increased automation and the integration of monitoring, management, and mitigation capabilities. Instead of arguing for one solution method over all the discussed challenges, the paper maintains that self-regulating approaches should be developed per-se given different organizations, cultural backgrounds, technical and financial resources, and regulation environments. The proposed framework should also provide improved capabilities to manage model risk during the deployment of AI models.

7.5. AI-enhanced Monitoring Systems

Board responsibility for risk management is essential in the risk framework. The board must review, evaluate and conduct oversight of all critical risk processes. Ultimately, it is management's responsibility for risk management and compliance. Management and senior management are responsible for implementing and maintaining the firm's risk policies and procedures. AI-enhanced monitoring systems support both management and board oversight functions. These systems can promote a more visual and higher assurance risk and compliance landscape and mitigate human cognitive biases and limited capabilities that may ignore the 80% of the 20% of risks that would not be picked up in a simple analytics notebook. The board is interested in, among other things, overseeing and reviewing high Severity designs and output from the AI systems. Testing of such devices by an independent group to confirm pre-agreed conditions and to understand parameterization would be one example of this oversight.

AI technical control weaknesses such as data limitations, model limitations, and design and output issues can cause failure in AI systems producing low-quality output. For non-AI systems, control weaknesses such as integrity and misuse can fail non-AI systems producing unusable output. The credit and other risks of low-frequency high-impact items and AI non-compliance have been increasing over time. Given the weaknesses inherent in AI systems, moreover, many unanswered questions exist as to how the largest credit books mitigate model error risks. Artificial Intelligence is regaining prominence and becoming a C-level corporate topic globally. Credit and compliance considerations with initial pilot implementation in high caution but high-benefit areas would apply. Such initiatives would double win on compliance and risk-adjusted returns along with thought leadership in these two high-stakes implementation challenges.

Cyber risk is also a major high-frequency low-impact risk. It is getting more and more challenging, and many flaws may go unnoticed despite robust monitoring systems. How threat intelligence is obtained, how often monitoring systems are updated, and how false positives and false negatives are investigated and understood are key questions in providing assurance. Manual processes surrounding cyber monitoring systems should also be reviewed. Excessive reliance on tools with compliance keeping up with regulation around the world may miss a more complete view of the risk. Robustness tests and stress tests may be valuable in the AI/ML space but are more difficult to implement. It is crucial to know what limitations or weaknesses in the AI/ML monitoring systems you do not know to cover gaps left by human ignorance. Nonetheless, tuning of cyber monitoring systems should be validated due to the extent of manual handling of human oversight beyond basic wrongful handling logic or ethical concerns on issues such as segregation of duties being outside Detection Joiners versus External Hackers.

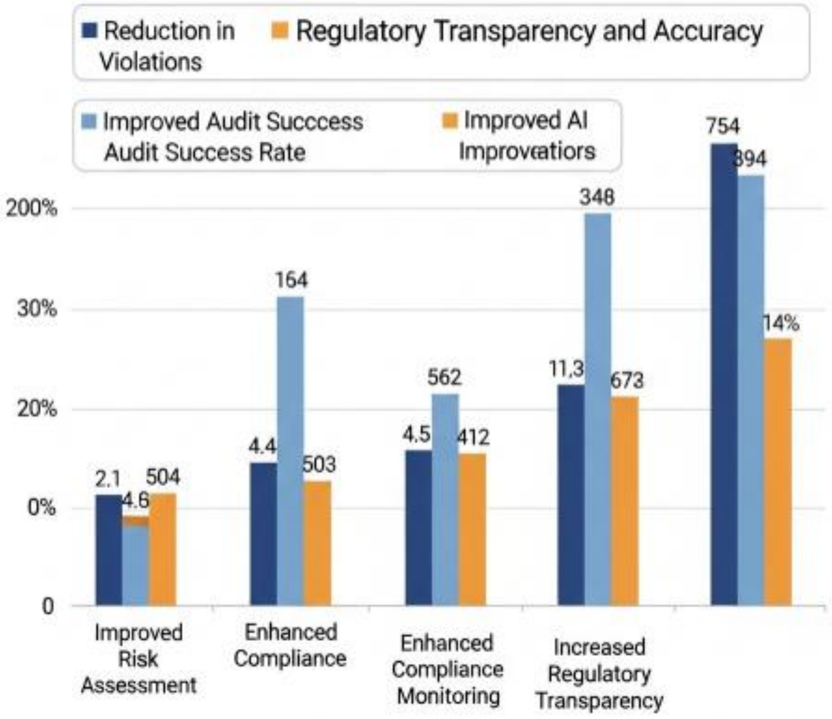

Fig 7.3: Achieve Regulatory Transparency and Accuracy

7.5.1. Data Collection and Integration

Data from a wide collection of sources play an important role in risk and compliance monitoring, including bank internal systems, communication records, and external news articles. Financial service companies typically maintain highly complex systems in accordance with the specific characteristics of various business lines. An application system may provide multiple services serving the same purpose but designed for a different client, such as SME loans or credit cards. Helping institutions identify useful information in these complex internal infrastructure systems requires additional efforts.

In this situation, Natural Language Processing (NLP) technology can be useful. The modality of this kind of data is mostly text. Multimedia data has an increasing importance. Audio records collection is common in KYC systems or trading rooms. Extracting and interpreting the voice record of the dialogues is more challenging yet still strived. Subsequently, the developed feature extraction models will be further integrated into the existing knowledge systems of banks, where a comprehensive data platform will be built. External data can come from different channels, including news analysis agencies, social media, and specific domain sources. For example, beyond standard news articles, the service for interpreting the news content of the companies involved in the market manipulation or scanning online posts to identify reputational risks in a specific time range can help financial institutes self-review over regulatory compliance. Such external news articles are naturally provided by diverse media companies and chained with complex information sources, targeted audience, and channel efforts in providing the information. It is essential to integrate various textual news articles, interpret the content, and build meaningful parameters on which the institutions can evaluate financial service candidates.

7.5.2. Real-time Monitoring and Alerts

An ingenious sophistication of AI-enhanced risk and compliance monitoring solutions is the division of data into risk classes and cohorts. The key question is whether it is necessary to assign risk classes to data before monitoring. A cohort is a group that uses a common set of monitor events for a disclosure period, which can be based on cohort characteristics. A risk class is one of the pre-defined risk classes assigned to emails, chats, transactions, etc. by AI-enablement processes. AI engines use classification techniques to assign risk classes to records, which can be pre-defined by compliance officers or risk specialists. The cohort and risk class information are essential for leverage risk and compliance monitoring systems, as they indicate whether additional filtering or monitoring improvements are required.

Under the cohort and risk class information mechanism, all the monitors that have been actively reviewing the monitors in parallel can be assigned to an incoming record or a defined cohort independently. Essential risk and compliance events matched with specific criteria are built to create corresponding alerts. An alert or flagged record means that compliance teams should examine incoming records in detail. All those alerts can be monitored in a workflow system called documented monitoring. For regular reviews, authorities can design routines for records and periodic stress tests and simulated monitored events disclosure to monitor the efficiency and accuracy of the monitoring system.

7.6. Improving Transparency with AI

Transparency in AI models is a crucial need for financial institutions aiming to ensure compliance, trust, and reduce risk exposure. Increasing transparency poses challenges to various financial services AI applications, including compliance, risk detection, and anti-money laundering, among other applications. With many AI-related questions unanswered, financial institutions are left with little understanding of how to ensure compliance and guarantee transparency. Such questions will continue to be frequent and important in areas such as selecting tech vendors, determining what level of transparency and explainability is needed, studying use cases on model exposures, sharing AI model insights with regulators, and assessing the transparency of existing models before adoption. Only with increased transparency of AI-enabled systems can the governance, policies, and control frameworks of financial services institutions adapt to mitigate risks. Without transparency, heightened scrutiny is expected from the public and regulators, which may hinder the growth of AI in the financial sector. Governance and regulatory solutions that enable transparency are crucial given how challenging the need is. It can be sophisticated and variety-driven, reflecting the sophisticated and diverse nature of AI models. AI transparency can manifest itself in several alternative manners, including (1) disclosing the potential model risks and data issues at the acquisition stage; (2) supporting due diligence and testing with detailed data, model, and design descriptions; (3) determining the need to share information with regulators; (4) allowing regulators to audit how code is implemented to ensure compliance; and (5) addressing the auditability of outputs by regulators post-model deployment, including the ability to rerun models, conduct sandboxes, and provide audit trails for output verification. There is also substantial model diversity within a particular application. Different AI techniques have different algorithms and data designs based on the risk, need, and characteristics of the application domain, and transparency should reflect those diversities. Solutions for transparency governance should acknowledge that AI models are used within a broader governance and regulatory framework that governs how to deal with model risks, including the types of data used, risk appetite, acceptable risk levels, governance roles (first, second and third lines), and sensitivity testing.

7.6.1. Data Visualization Techniques

In a digital world, data is vital to all firms and controls for behavioral outcomes encapsulated in data are core to regulatory systems. Risk and compliance monitoring systems anchor risk mitigation activities, including clarifying controls, evaluating effectiveness, and remediating weaknesses. However, firms are overwhelmed by data-laden information, as data growth outpaces the ability to monitor risks and compliance. Left uncoordinated, information overload has negated efforts to enhance risk and compliance systems, leading to misses on events and opportunities. There is also a blind spot in oversight of trust but verify perspective deeper in the Risk and Compliance obligations. In particular, economic substance regulations, taxation, fraud detection, insider trading, disclosure obligations, trigger-free allowance go unnoticed in existing systems. At the same time, there is a need to upscale threats following the growing sophistication of frauds, ransomware, crypto-schemes, and money laundering. Firms have thousands of systems monitoring millions of alerts daily, uncoordinated across businesses and locations. Enabled by low-code and no-code Natural Language Processing, Graphs, and machine learning, augmented capabilities built on cloud infrastructure incorporate techniques centered around a human. Information overload is addressed through smart data insights and smarter machine insights, which can complement ESG, Compliance, and Cyber initiatives. A monitoring newsroom provides a horizontal view across information domains and pipelines to aid traditional workflows as well as automated investigation. The system generates in-depth analysis narratives and condenses information for effective stakeholder engagement. In addition, trust but verify governance of alert outcomes adopts explainable modern graph-techniques across administrative records and public data. Inspection of patterns and relationships form the basis of ground-truthing and deselecting irrelevant alerts, allowing for less noise in systems.

7.6.2. Reporting and Audit Trails

Besides identifying risks in real-time, it is essential to track the upcoming examples and monitor the actions taken on them. Regulatory authorities request audit trails for several reasons: a comprehensive and time-stamped view of possible misconduct, an effective monitoring solution, detection of emerging models of misconduct, a guide on why a specific decision was made (i.e. ‘explainability’). There are several approaches on how to be compliant at the same time while developing these tracking and reporting features. Tracking relevant variables can reduce risk-exposure in this area and hold evidence in case it would be of value. Decisions can be conditioned and queried as easily as raw data can as well. Provided that a structured format of key evidence is kept, auto generated compliance documents can easily be created. Nonetheless, submission of compliance documents is time-consuming in a multi-regional area spanning several time zones. Whenever a compliance document is due, a designated user must do extensive searches for relevant events, decisions, risk assessments, and justifications. In addition, users are expected to have expert domain knowledge in different areas, risking a missed event of regulatory value. This reason alone provides motivation to build an automated solution. An in-house compliance-auditor can periodically investigate the approaches taken across different teams (or regions), comparing them against known expectations and adjusting them accordingly. Informal approaches can also be more efficient and accurate, thus resulting in less time and manual error.

7.7. Conclusion

Regulatory compliance has become a top priority for financial institutions after a series of scandals, unprecedented monetary stimulus, and equity market turbulence worldwide. These institutions are subject to risk and compliance monitoring by regulators armed with an extensive toolkit. They must construct and maintain a compliance monitoring system for this purpose. However, it is challenging to build a reasonable risk and compliance monitoring system due to regulatory complexity and sophistication, and the possibility of a myriad of violations requiring inference from incomplete audit trails or explicit manipulation trail management logging of all phenomena of interest.

Due to the increasing complexity of adhesion activities and the continuous evolution of regulations and standards, rules and mitigations are proliferating. Even for common offices and trade facilitations, the regulatory compliance monitoring system is far from comprehensible. Most rules are established using transaction-level attributes, which makes it difficult, if not impossible, to make the rules comprehensible and to take appropriate measures even if the rules remain understandable. Most importantly, rules and mitigations do not evolve comprehensively or uniformly. When new variants of trading algorithms or compliance measures are specified, existing monitoring systems usually fail to trace the changes, leading to more compliance monitoring holes. Precise identification of violations is still a theoretically unresolved but practically urgent problem.

To tackle the challenges, this work presents an intelligent risk and compliance monitoring system framework to enhance regulators' risk and compliance monitoring systems. Innovative cascaded general probe technologies are proposed to discover compliance violations and extract the non-compliance processes from the trading and investigatory trails of potentially non-compliant trading algorithms. This framework features: improved risk discovery using a transduction-based strategy for semi-supervised evaluation and sophisticated violation sampling; comprehensive risk identification using situationally aware probes; shifts from evaluating the suspicious algorithms to comprehensive enhancing bids including a pipeline for comprehensively extracting potentially non-compliant trading processes.

7.7.1. Future Trends

Organizations, regulators, and researchers are looking towards innovative solutions for tackling growing data risks in R&C. AI-based systems have shown promise in the area, providing sophisticated new approaches for improved automation, vigilance, and intelligence. Despite the potential of these new technologies, the limitations and risks of AI-based systems must be taken into account, leading to the development of a self-regulating AI system architecture for risk monitoring. This architecture allows AI-based compliance systems to be monitored in an automated and real-time manner, while simultaneously maintaining management oversight over the AI system's development and deployment phases. Embedding regulatory guidance within the individual AI compliance models prevents future compliance failings. The design choices and challenges of implementing the architecture are discussed, as combined AI regulation and guidance approaches provide improved modeling capabilities.

Self-regulating AI models for risk and compliance monitoring designed for organizations to assess ML and AI systems across a range of use-cases are introduced. It is argued that AI-based compliance systems should be held to the same technological, managerial, and reporting standards as conventional monitoring systems. The ability to tap into vast behavioral data of monitored models and up-to-date guidance provided by real-time regulation and compliance technology is created. A 'robotic lawyer' able to provide compliance advice for a variety of AI systems independent of the model architecture is one application of this framework. The increasing sophistication of AI-based monitoring systems warrants a move away from only qualitative human-assessed compliance requirements and assessment reports. Silver-bullet solutions provided by AI can dynamically transform R&C failings into recommendations for sweeps and tune AI systems remotely.

While truly autonomous compliance systems remain unattainable, self-regulating AI architectures can provide assurances over the input data, model development, and deployment safeguards. The challenge of embedding management and human oversight is addressed, acknowledging the complexity of modern systems and highlighting areas in AI design that can be influenced. Management oversight becomes more important than ever, as AI systems mature from a network of systems to a connected mesh of agents. Increasingly deep neural nets that autonomously explore the input feature space for a new learning task and dataset are discussed, arguing that at a higher level, discretion on regulatory matters such as wind-down is retained by the organization.

References

Anderson, T. (2025). AI and the evolution of financial intelligence. In The New Frontiers of Financial Services (pp. 23–41).

Becker, J. L., & Sharma, N. (2025). Ethical frameworks for AI in automated lending. In The New Frontiers of Financial Services (pp. 128–141).

Brandt, S. (2025). Predictive analytics and credit risk modeling. In The New Frontiers of Financial Services (pp. 56–70).

Chen, Y., & Lopez, F. (2025). Natural language processing in investor sentiment analysis. In The New Frontiers of Financial Services (pp. 172–190).

Desai, M. (2025). Redefining customer value with AI-driven personalization. In The New Frontiers of Financial Services (pp. 92–110).