Enhancing Compliance Monitoring with NLP and Semantic Analysis Techniques

Pratik Chawande
Independent Researcher, Dallas, Texas, USA

* Corresponding Author: **Pratik Chawande**

Article Info

ISSN (Online): 2582-7138
Impact Factor (RSIF): 7.98
Volume: 06
Issue: 01
January-February 2025
Received: 09-11-2024
Accepted: 11-12-2024
Published: 08-01-2025
Page No: 2183-2189

Abstract
The dynamically increasing trend of the regulation requirements and the succeeding intensification of the amount of transactional and communication data have posed critical questions with the observation of the conformity inside the companies. Financial institutions, medical care providers, and other institutions that are under control are also under pressure to identify suspect actions and decrease compliance expenses and efficiency. Although it might seem that old rule-based systems of monitoring are not so young anymore, they are getting less efficient to combat these challenges. These systems are based on programmed limits, rules and keyword recognition which tend to produce too many false positives which produce operational inefficiencies and regulatory risks.

Possible alternatives can be provided by the recent developments in natural language processing (NLP) and semantic analysis. These procedures assist systems to perform linguistic context, intent and unstructured data examination in a superior way. The majority of the latest advances in word embeddings, transformer models that are based on domain-specific financial and compliance purposes and applications have triggered access to contextual and scalable monitoring. NLP could offer deeper meaning of messages and transactions under the element of going beyond the concept of identifying keywords and ultimately narrowing down the number of false alarms and enhancing effectiveness of compliance control.

In this paper, monitoring architecture is suggested, and it includes a group of transactional and communication streams of information along with a combination of artificial intelligence (AI) and machine learning (ML). To be exact, semantic role labeling, knowledge graphs, and transformer embeddings are used to offer further opportunities to detect and lessen the load of compliance departments. A part of the work of the research is provided in the developed system architecture, critical survey of the current methods, and discussion of the application in the industry. The case study of HSBC, Dynamic Risk Assessment program, and JPMorgan, COiN system shows how powerful AI-compliance systems are revolutionary.

DOI: https://doi.org/10.54660/.IJMRGE.2025.6.1.2183-2189

Keywords: Algorithms Artificial Intelligence (AI), Machine Learning (ML), Regtech, Anomaly Detection, Knowledge Graphs Compliance Monitoring, Natural Language Processing (NLP), Transaction Surveillance, Semantic Analysis, Explainable Ai, Financial Crime Prevention.

1. Introduction

The financial industries are controlled by compliance monitoring, which has proven to be one of the most resource consuming functions. The current regulatory environment is becoming a challenge; companies are being audited more and fining more in case of noncompliance. The UK Financial Conduct Authority (FCA) fined HSBC 64 million pounds as an indicator, over its

anti-money laundering (AML) activities and this fact underscores the dangers of not having an effective internal control [12]. It is estimated that the cost of compliance and risk management in the world is still increasing and companies are willing to spend billions of dollars to fulfill the demands of the regulations as the consulting firms like Deloitte estimates [13]. This is costly, not to mention operational inefficiencies, given that compliance staffs may use massive resources on false positives and hand-checking of alerts.

The conventional compliance monitoring system depends on the outdated measures in the system like manual check of the rules, identification of keywords and surveillance threshold. As much as these systems have the capacity to raise an alarm whenever an unusual transaction or suspicious phrase is realized, the systems are unable to understand the context of the transactions. Consequently, the rule-based approaches do not easily differentiate the innocent action and a truly suspicious action [3, 16]. Periodically, on indicative basis, periodic notifications can be shown as the outcome of legal foreign transactions, or general employee communications, though the technology of the time considered them as workable violations and inundated compliance officers with unnecessary inquires.

Regulatory technology (RegTech) has raised a new stream of interest in finding out the strength of AI and ML to transform compliance operations. Scientists and professionals also specify that the next stage of the evolution process of risk management will be the monitoring with the help of AI [15]. Unlike the rule-based system, AI can learn and adjust to changing behavior and recognize nuanced patterns within the different streams of data. Precisely, the NLP techniques allow the intent of communications, extraction of entity in unstructured text, and graphical semantic relationships among transactions. The said developments help compliance teams with prioritizing the alerts and working on the cases of higher risks.

Despite these advancements, there is one more significant problem which is urgent, and that is the fact that the majority of the available compliance systems lack contextual awareness [6]. They are able to pick suspicious key words or suspicious activities but in the majority of cases they fail to see the bigger picture of messages or deals. The other instance is that an insider information is hidden by a trader whose wordings are rather vague to attract attention in a keyword driven system. However, contextual NLP procedures would be in a position to locate intent through research of the semantics of nearby text.

The purpose of this paper is to propose a full-scale monitoring architecture that would make use of NLP and semantic analysis when dealing with compliance processes. The three contributions in the work are the survey of the current compliance monitoring techniques, the constraints of the previous systems, and the opportunities of NLP; it suggests an architecture, which includes the semantic analysis, machine learning, and explainability features in compliance monitoring; and it evaluates the practical applications in the domain, providing the examples of the major financial institutions, such as the HSBC and JPMorgan [8, 9].

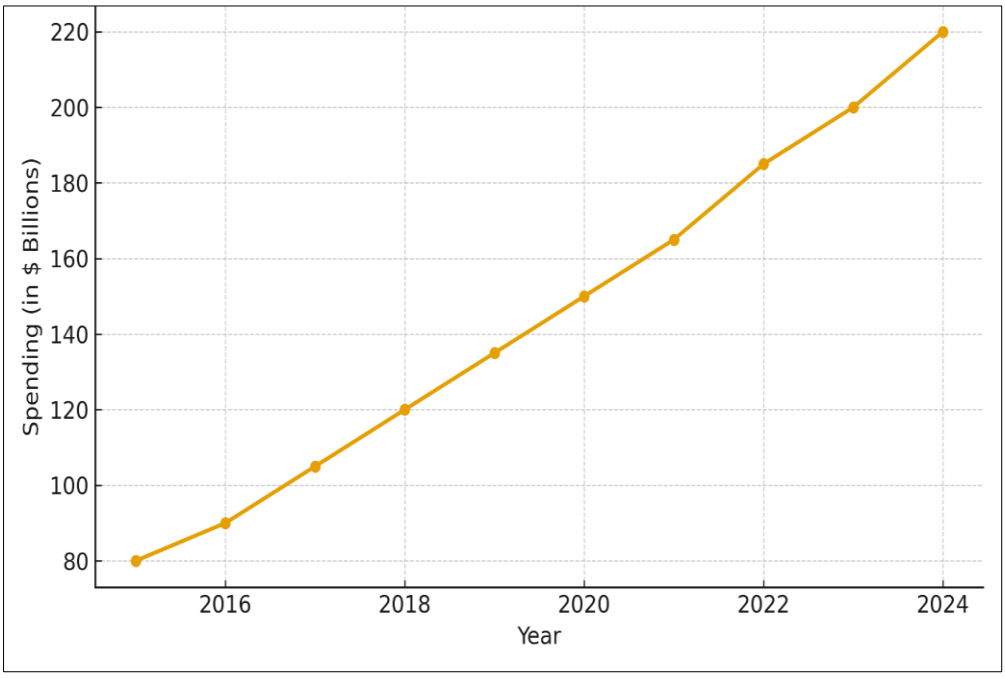

Fig 1: Illustrate the global compliance spending trend using Deloitte's data [13], providing a quantitative perspective on the urgent need for more cost-effective and scalable monitoring solutions.

2. Literature Review

2.1. Traditional Compliance Monitoring

The former method of compliance monitoring was rooted on the predetermined rules and limits and the identification of suspicious activity. They may include financial institutions having systems that are used in the AML sector to indicate transactions that exceed a particular amount of money, or after transfer of funds on risky jurisdictions, or after scanning of communications containing particular keywords [3]. Although such systems are effective at the low-level, they are not able to keep up with the evolving risk patterns and tend to generate significantly large number of false positives. Among the negative aspects that they should list among their limitations, one must mention the inability to determine the difference between a legitimate business operation and a truly criminal behavior that can overwhelm the compliance

departments and reduce efficiency of business [12].

The other weakness is the limited scope of intent interpretability. Context-blind rule-based monitoring is a common phenomenon i.e. it might be able to detect transactions which meet a certain criterion but not the intent behind such practices. As an example, large global transaction may be considered a red flag on its own but in the context may form a formal transaction of a company. This kind of a poor contextual interpretation can lead to false positives, which, in its turn, reduce trust in the monitoring system [16].

In addition to the inefficiencies, the legacy systems cannot be scaled. As the transaction volumes increase the existing systems are not able to increase in line with the increase and consequently lead to spamming of alerts. This scalability gap also indicates that intelligent and adaptive approaches to monitoring systems are important in considering contextual and semantic analysis.

2.2. NLP in Finance & Compliance

NLP is a relative entry to the unstructured data processing particularly in the compliance area where information on communication, reports and financial data is required to be computed massive amounts of data. The text representation approach, such as Word2Vec [2] or transformers-based model, such as BERT [1], has changed the form of text representation, syntactic and semantic meaning. The models assist the systems to perceive the linkage among words, locate a context and the remaining downline processes, such as classification and sentiment analysis in a narrower context.

The NLP has been applied in the text mining processes of financial compliance like news article analysis to detect market sentiments, identify regulatory filing actions as well as detect news article analysis [4]. Such applications demonstrate that NLP can not only be capable of matching the keywords, but possibly even of semantic matching, and it can be very useful in the area of compliance monitoring. The illustrations are that, the suspicious communications between the workers or among traders can be evaluated not just based on certain keys but with allusions to the secret patterns that may be correlated with collusion or may be directed at controlling the markets [6].

Entity recognition is the other significant NLP application in compliance. Systems can be used to auto-extract named entities (e.g. individuals, organizations and financial instrument) in text data. The latter is particularly required to estimate the beneficial owners, the relationship or counterparties of the high-risk entities. It is also aided by semantic search because the compliance teams can search the large text corpora to capture the information that is contextually related but not through the process of employing the keywords. This way, the compliance teams will be in a position of increasing their ability to identify the not obvious risks and foresee.

2.3. Semantic Analysis & Knowledge Graphs

The semantic analysis is the development of NLP since it is concerned with the correspondence between objects and the meaning of the text in even more abstract forms. According to this, the intent may be provoked by semantic analysis and as the associations are usually neglected in rule-systems, they may be uncovered. To illustrate the point, the role of actors is stipulated by the names of semantic roles (e.g., sender, receiver, intermediary) that allows retrieving an essential piece of information on the suspicious activity [5].

Knowledge graphs have become powerful instruments of AML detection. The knowledge graphs are suitable in the identification of the intricate patterns of the financial crime since they model the entities and the graph relations as nodes and edges respectively. It is shown that a combination of the two knowledge graphs with machine learning can help to enhance the process of the detection of money-laundering networks by revealing any hidden links between the transactions [7]. This strategy will especially help identify layered transactions, shells companies or collusive patterns of communications which are impossible to achieve using the old tools of monitoring.

Moreover, it has semantic analysis and domain specific ontologies, which, combined with them, improve readability and transparency. Ontologies give standard sets of vocabularies of financial transaction that offer systems to rationalize dubious designs in a steady manner with regulatory taxonomies [5]. This is also accompanied by the contextualization and law-abiding AI-driven systems.

2.4. Explainability & Regulatory Alignment

The explainability is also one of the significant traps along the way to the AI-based compliance monitoring. The other stipulation that regulators put forward is that the financial institutions must also show that they have operating system besides showing that the decision made by the system is transparent and auditable. The institutions will not be able to have the regulatory approval of AI-based monitoring solutions unless it can be explained. Regarding form, researchers have suggested explainable artificial intelligence (XAI) models, which provide the elaboration to the model decisions, in a manner that would allow the auditors to discover the notifications to the evidence [10, 11].

The explicability of the data analysis is especially significant in the cases of vicinity stakes where non-conformance may be accompanied by the colossal financial punishment. The AI-based solutions can be credible by the compliance departments making them understandable in the form of easy interpretations of post-hoc explanations. A few instances of methods of demonstrating accountability consist of [10] decision trees, attention heatmap on transformers, and counterfactual explanations.

The other cause is regulatory alignment. The regulators are becoming more concerned with the AI-compliance and have mandated that companies must adopt efficient governance infrastructure, according to reports by Deloitte and PwC [13, 14] and others. The latter structures justify the need to make the data privacy, simplify the bias, and auditable. Lack of adherence to these requirements does not only enforce efficiency of compliance, but may also result into reputational and monetary losses to institutions.

Table 1 give a comparative report on the NLP-based and rule-based compliance system and project which mentions that there is a difference between the two in the aspect of scalability, false positive rates and context sensitivity [16].

Table 1: Comparison of Rule-Based vs. NLP-Driven Compliance Monitoring Systems

Feature/Aspect	Rule-Based Systems	NLP-Driven Systems
Flexibility	Limited to predefined rules; struggles with unstructured data [3]	Adapts to diverse and evolving communication patterns [4, 16]
Scalability	Difficult to maintain as compliance rules and regulations evolve [3]	Scales efficiently with machine learning and semantic processing [16]
Accuracy in Detection	Prone to false positives due to rigid keyword matching [4]	Higher accuracy through contextual and semantic understanding [16]
Adaptability to Context	Poor contextual comprehension; requires manual updates [3]	Learned contextual data trained dynamically [4, 16]
Cost of Maintenance	High due to frequent rule updates and manual oversight [3]	Lower costs of doing business in the long run as a result of automation and adaptive learning [16]

3. Proposed Monitoring Architecture

The mere speeding up of unorganized financial and communication content leading to the requirements of both compliance monitoring systems required to meet the soaring regulations requirements and at the same time remain efficient in its operations. The traditional rule-based systems are not scalable to the extent required and they do not offer a sense of context that requires the incorporation of an improved architecture that relies on the use of both natural language processing (NLP) and semantic analysis [3, 12]. The part proposes the need to monitor architecture, which involves the inclusion of several AI/ML parts to create a situation-conscious, explainable, and regulator-friendly compliance framework.

3.1. Design Principles

The basis of the proposed monitoring system is three principles namely scalability, explainability and regulatory compliance. Scalability implies that the system is capable of handling immense amounts of transaction and communication information in the financial institutions, healthcare organizations and telecommunications networks. The distributed computing frameworks and cloud-native architecture can be used to horizontally scale the solution to handle millions of transactions, chat records in near real-time [5].

Explainability is the whole issue of regulatory acceptance, regulatory compliance officers must understand the logic of alerts. The system integrates explainable AI (XAI) modules, which are applied to provide explanations to suspicious activities that are detected by machine learning models [10]. The reasons are very fundamental in fulfilling audit requirements and transparency. Finally, strong anonymization, data protection, and model training procedures following the principles of privacy [11, 14] must be adhered to by the General Data Protection Regulation (GDPR) and other data protection policies. All these design principles will work together to provide some balance between the requirements of the operations and ethics and regulation requirements.

3.2. Architecture Layers

The architecture has various layers where each layer has a limited number of responsibilities that are required to reach the efficient compliance monitoring.

Data Sources Layer. The system handles both structured and unstructured information, which is submitted by various sources i.e. financial transactions, email messages and the instant messaging systems [6]. The implementation of such in the form of a multimodal will ensure that all risks of all the three or more kinds of transactional fraud and insider communications will be monitored through a single pipeline.

Preprocessing Layer. As a step to analyse the incoming data, they are anonymised so as to maintain the personally identifiable information (PII), and tokenised so as to analyted via an NLP-based approach. They are highly beneficial when it comes to creating domain specific vocabulary and multilingual data using the existing form of tokenization such as the sentence piece tokenization and the byte-pair encoding tokenization [1].

NLP Engine. A system-focused on the contextual embeddings is the center of the system, which is built on the models of Word2Vec [2], and BERT [1]. These embeddings can be used to detect textual semantic intent such as whether a conversation is signaling money laundering or is an insider trading conversation. The NLP engine is capable of exceeding the matching of the keywords and therefore attaining subtle meanings, which would not have been the case with the previous monitoring systems.

Semantic Layer. It relies on knowledge graphs [7] and regulatory taxonomies [5] in order to provide financial transactions with perspective. One of them is that mapping an abnormal transaction to a high-risk entity graph, it is possible to conclude whether the specified transaction can be regarded as legitimate or not. Semantic layer will also be used to identify occurrences and align them with regulatory models, i.e. AML guidance or GDPR requirements.

ML/Anomaly Detection Layer. Two of the deviations the developed models have identified in the case, the ones that have been identified are the transformer-based classifiers [1] and semi-supervised learning models [16]. Semi-supervised learning also does not necessitate in large amounts of labelled training in comparison to fully supervised models that not necessarily exist in the compliance domains.

Threat Scoring Layer and Notification. Finally, the compliance officers are offered the risk scores in the form of flagged anomalies. The human-in-the-loop design will maintain the system highly expert validated and having less risk to regulation and is responsible [10].

3.3. Algorithmic Components

The geometry goes into complete algorithmic in making the contextual understanding and the consistency of the regulation more intense.

Context-Sensitive Scoring of similarity. The system is implemented using similarity scores of unnatural communications with known high-risk patterns by word embedding, like Word2Vec [2]. It is the most convenient process in small collusion or coded message detection.

Generative AI Explanations. The AI models of the generative natures generate the natural language summaries that explain the intent of the purpose of raising an alert. An example of

this can be muting a suspicious e-mail of which one can do that due to the use of a foreign account in a reputable tax haven [5, 15]. These kinds of descriptions persuade them more and allow the auditors to know the logic behind the system.

Explainability Modules. Explainable AI systems [10, 11] are the systems where visualization and explanation of events that are flagged is understandable. These modules are especially crucial in the situation of regulatory issues on the black-box artificial intelligence models and the audit standards.

On the whole, this architecture puts compliance monitoring to another dimension and employs NLP and semantic technologies to create regulatorily compliant, context sensitive and scaled system.

4. Practical Industry Applications

The proposed monitoring framework is not purely theoretical because it aligns with the practical applications in the financial services sector, healthcare sector and telecommunications sector.

4.1. Financial Services

The field of financial industry may be regarded as the most developed area in terms of the implementation of AI/ML-driven compliance monitoring. The Dynamic Risk Assessment platform implemented by HSBC is founded on the idea of applying the machine learning and NLP algorithms to detect the patterns of money laundering in a more precise way [8]. This system has been able to reduce false positives and devise proactive risk assessment. Similarly, JPMorgan has developed the COiN platform, where the complicated financial documents and transactions records analysis are automated [9]. The JPMorgan has been able to extract semantic meaning using legal contracts and communications with clients that have made compliance review processes less onerous and time-consuming processes that required thousands of human hours.

These instances illustrate that the big institutions employ NLP and semantic analysis to address regulatory requirements and reduce the workload of the operations. The experience of these kinds of implementations has been directly applied to the design of the proposed architecture.

4.2. Healthcare and Telecom

In addition to finance, compliance tracking is a mandatory activity in such sectors as healthcare and telecommunications. HIPAA and GDPR impose strict demands on healthcare organizations that handle sensitive patient data [11, 14]. The communication between medical professionals is tracked by NLP-based systems that can make sure that the data-sharing habits do not violate privacy laws.

Monitoring insider communication is important in telecommunications to stop the misconduct of corporations and the protection of privacy of customers [6]. NLP models can identify the attempts to breach the security measures or to exchange confidential information by analyzing the chat logs and emails.

4.3. Benefits

These industries have the practical gains of the use of NLP and semantic analysis. To start with, it has a considerable decrease in false positives as opposed to previous rule-based systems [3, 8]. This lowers fatigue of compliance officers and the resources can be used on actual risks. Second, clarifiable AI modules are more likely to help organizations respond to audit requests at a faster pace, being able to offer clear explanations of why decisions to monitor were made [10, 11].

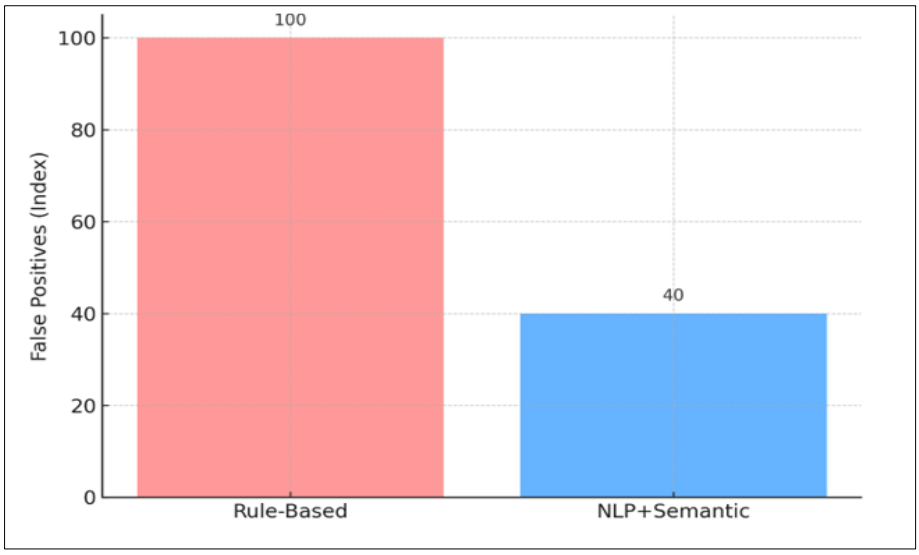

Fig 2: False Positive Reduction (HSBC Case Example)

The case example of false positive reduction at HSBC as presented in Figure 2 shows that the performance has improved compared to the traditional methods [8].

5. Discussion

The given architecture has a number of strong points, however, there are issues that should also be taken into consideration to be evaluated in a balanced manner. One of its strengths is scalability, which means that the cloud-based infrastructure can perform parallel processing of large datasets [5]. Another benefit is context sensitivity; embeddings, and semantic models allow distinguishing subtle patterns that are not recognized by a rules-based system [1, 2]. Also, automation decreases the cost of operations in an attempt to handle the economic strain of increased compliance costs [13]. In spite of these advantages, there are

some challenges. One of the key issues is model drift that is changing according to the new strategies of financial crime [16]. Models should be retrained and monitored on a regular basis to ensure effectiveness. NLP models also pose risks in terms of bias especially when trained on biased datasets [4]. These biases can cause excessive monitoring of some population groups or insufficient detection of new schemes of fraud.

The adoption of AI in compliance is of concern to regulators because of the issue of transparency. The explainability requirement is also high, and frameworks like XAI are critical to the alignment of regulations [10, 11]. There are also trade-offs of accuracy versus interpretability in the system. Deep learning models with high complexity can be more accurate but cannot be explained, whereas simpler models are more transparent, but less performant [13, 14]. The correct balance is still a challenging issue.

6. Conclusion

The paper has introduced a compliance monitoring architecture with the application of NLP, semantic analysis, and machine learning to overcome constraints of the traditional systems which are rule based. The architecture permits perceiving the context, scaling and regulatory compliance through the exploitation of embeddings, knowledge graphs as well as explainable AI.

The practical experiment in other areas such as finance and healthcare suggest the practical viability of such systems with certain institutions such as HSBC and JPMorgan already testifying that they have fallen to false positives by a wide margin and have also improved audit preparedness [8, 9]. Compliance is not a simple cost center, but a strategic enabler when used by AI/ML, which enables companies to deal with the risks of regulation, and make their operations efficient [13, 15].

Lastly, the combination of NLP and semantic analysis is an unheard of in compliance monitoring that offers a path towards more intelligent and transparent and globally sensitive regulatory practices.

The compliance monitoring will further be enhanced in the future with the emergence of developing AI techniques. Generative AI offers the opportunity of contextual compliance reporting, where the reporting of the regulatory reports is automatically generated, summarizing the anomalies and the reasons why [5, 15]. This reduces the number of workloads required to be done manually and improves interaction with the regulators.

The other direction that is geared towards ensuring that cross-border compliance issues are managed is multilingual monitoring. The NLP is used in upgrading multilingual transformers; however, this service transforms the transactions and communications between diverse jurisdictions [4]. The hybrid systems combining rule-based systems with AI models will also matter since they will be more flexible and readable [16]. In addition, edge-based real-time monitoring is also a recent development particularly in telecommunication and financial systems where latency is of primary importance [7]. When the light weight models are implemented in the network edge, this implies that the compliance risk is monitored in near real time without the centralized processing.

7. References

1. Devlin J, Chang MW, Lee K, Toutanova K. BERT: pre-training of deep bidirectional transformers for language understanding. In: Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies (NAACL-HLT); 2019 Jun 2-7; Minneapolis, MN. Stroudsburg, PA: Association for Computational Linguistics; 2019. p. 4171-86. Available from: https://aclanthology.org/N19-1423.pdf
2. Mikolov T, Sutskever I, Chen K, Corrado G, Dean J. Distributed representations of words and phrases and their compositionality. In: Advances in Neural Information Processing Systems 26 (NIPS 2013); 2013 Dec 5-10; Lake Tahoe, NV. Red Hook, NY: Curran Associates; 2013. p. 3111-9. doi:10.5555/2999792.2999959
3. Oztas B. Transaction monitoring in anti-money laundering. Comput Fraud Secur. 2024;2024(6). Available from: https://www.sciencedirect.com/science/article/pii/S0167739X24002607
4. Du K. Natural language processing in finance: a survey. Res Int Bus Finance. 2025;73:102533. doi:10.1016/j.ribaf.2024.102533
5. S, et al. Regulatory graphs and GenAI for real-time transaction monitoring [Internet]. arXiv. 2025 Jun [cited 2025 Oct 9]. Available from: [URL not provided]
6. Integrating natural language processing (NLP) in AML compliance and monitoring [Internet]. ResearchGate; [date unknown] [cited 2025 Oct 9]. Available from: https://www.researchgate.net/publication/380972184_Integrating_Natural_Language_Processing_NLP_in_AML_Compliance_and_Monitoring
7. Bakhshinejad N, Soltani R, Nguyen UT, Messina P, et al. Enhancing anti-money laundering systems using knowledge graphs and graph neural networks [Internet]. ResearchGate; [date unknown] [cited 2025 Oct 9]. Available from: https://www.researchgate.net/publication/387449610_Enhancing_Anti-Money_Laundering_Systems_Using_Knowledge_Graphs_and_Graph_Neural_Networks
8. HSBC. Harnessing the power of AI to fight financial crime [Internet]. HSBC; [date unknown] [cited 2025 Oct 9]. Available from: https://www.hsbc.com/news-and-views/views/hsbc-views/harnessing-the-power-of-ai-to-fight-financial-crime
9. Case study: J.P. Morgan "COiN" — AI in finance [Internet]. ProductMonk; [date unknown] [cited 2025 Oct 9]. Available from: https://www.productmonk.io/p/meet-coin-jpmorgan-s-efficiency-wizard
10. Desai H. Explainable AI models for financial regulatory audits [Internet]. SSRN; 2024 [cited 2025 Oct 9]. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5230527
11. Explainable AI for regulatory compliance in financial and healthcare sectors — a comprehensive review [Internet]. Int J Adv Eng Manag. 2025 [cited 2025 Oct

9]. Available from: https://ijaem.net/issue_dcp/Explainable%20AI%20for%20Regulatory%20Compliance%20in%20Financial%20and%20Healthcare%20Sectors%20%20A%20comprehensive%20review.pdf
12. The Guardian. HSBC fined £64m for failures in anti-laundering processes [Internet]. The Guardian; 2021 Dec 17 [cited 2025 Oct 9]. Available from: https://www.theguardian.com/business/2021/dec/17/hsbc-fined-64m-failures-anti-laundering-fca
13. Deloitte. AI risk and approaches to global regulatory compliance [Internet]. Deloitte; [date unknown] [cited 2025 Oct 9]. Available from: https://www.deloitte.com/uk/en/Industries/technology/perspectives/ai-risk-and-approaches-to-global-regulatory-compliance.html
14. PwC. Managing the risks and opportunities of generative AI [Internet]. PwC; 2023 Oct [cited 2025 Oct 9]. Available from: https://www.pwccn.com/en/risk-assurance/managing-the-risks-and-opportunities-of-generative-ai-oct2023.pdf
15. S, et al. AI-powered regulatory technologies transforming compliance [Internet]. SSRN; 2024-2025 [cited 2025 Oct 9]. Available from: https://papers.ssrn.com/sol3/Delivery.cfm/5349014.pdf
16. Bakhshinejad N, Soltani R, Nguyen UT, Messina P. A survey of machine learning based anti-money laundering solutions [Internet]. ResearchGate; 2022 Oct [cited 2025 Oct 9]. Available from: https://www.researchgate.net/publication/364326902_A_Survey_of_Machine_Learning_Based_Anti-Money_Laundering_Solutions