Two-Level Model Information System for RegTech-Monitoring the Reporting Entities in Risk-Based Supervision

Ganna Panasenko[*] [1, 2], Viktoriia Hurochkina [3,2†], Serhiy Shtovba[4,5†]

[1] State Tax University, Universytetska Street, 31, Irpin, Kyiv region, 08200, Ukraine,

[2] Institute of Business and Technology, Star Lane, 1/5, Kyiv, Ukraine, 04078, Kyiv, Ukraine,

[3] University of Zielona Góra, Zielona Góra, Licealna 9, 65-417 Zielona Góra, Poland,

[4] Vasyl' Stus Donetsk National University, 600-richya str., 21, Vinnytsia, Ukraine,

[5] Vinnytsia National Technical University, Khmelnytske Shose, 95, Vinnytsia, Ukraine.

Abstract

This study examines the concept of an information system of the RegTech platform type, designed to monitor data on primary financial supervision entities in order to enhance the effectiveness of risk-based supervision. The methodological framework of the study comprises system analysis, conceptual modelling, functional-architectural design, and benchmarking against international approaches to supervisory technologies, machine-readable reporting, and advanced analytics in anti-money laundering and countering the financing of terrorism. The underlying problem stems from the fragmentation of information flows, the aggregated and templated nature of reporting, time lags in data acquisition, and the weak integration of structured and unstructured sources. A two-level implementation model is proposed: the first level characterises the transition to granular data and shared data models, whilst the second level reflects the mechanism of data flow integration in near real-time using natural language processing, machine learning, network analysis, and risk scoring. The study results in a coherent system architecture encompassing modules for data unification, profile enrichment of supervised entities, early warning, risk visualisation, and interagency cooperation. The scientific novelty lies in combining regulatory reporting, state registries, sanctions lists, and market data within a single analytical loop tailored to supervisory needs. The practical value lies in reducing information asymmetry, shortening supervisory response times, and establishing a solid foundation for predictive analytics and early risk detection.

Keywords

RegTech, information system, financial monitoring, risk-based supervision, AML, risk warning.

1. Introduction

Digitalization of the financial sector, the growing volume of regulatory data, and the emergence of new types of risks are changing the very logic of state supervision. The traditional model, relying on periodic reporting and selective manual verification, is increasingly proving insufficient for the timely detection of anomalies, network connections, behavioral patterns, and cross-sectoral risk transfer. In international practice, this shift is described by the concept of RegTech (Regulatory Technology) – which represents a set of innovative technologies (artificial intelligence, big data, cloud technologies) used to automate compliance processes, risk management, and regulatory reporting in financial and non-financial sector companies (reporting entities). They help reporting entities comply with legal requirements while reducing costs and increasing the efficiency of transaction verification [1, 3, 12]. At the macro-institutional level, the quality of regulation is also considered one of the core characteristics of governance capacity [11].

The problem manifests itself with particular urgency in the field of anti-money laundering and countering the financing of terrorism (hereinafter referred to as AML). In this domain, state

[1] RS-2026: Resilient Systems: Secure Digital Technologies and Critical Infrastructure, June 30, 2026, Drohobych, Ukraine

[*] Corresponding author.

[†] These authors contributed equally.

panasenko@kibit.edu.ua (G. Panasenko); v.hurochkina@wez.uz.zgora.pl (V. Hurochkina); s.shtovba@donnu.edu.ua (S. Shtovba).

0000-0002-6743-6728 (G. Panasenko); 0000-0001-8869-0189 (V. Hurochkina); 0000-0003-1302-4899 (S. Shtovba).

authorities simultaneously operate with large volumes of transactional and non-transactional data, suspicious transaction reports, corporate information, sanctions lists, judicial information, open market sources, and news feeds. As research shows, the combination of structured and unstructured data, alongside the application of network analysis, natural language processing, and machine learning, significantly expands the capabilities of competent authorities to detect suspicious connections, anomalous behavior, and new risk patterns [2, 4, 5]. At the same time, international experience demonstrates that regulatory reporting often remains complex, costly, inflexible, and overly tied to specific use cases. Problems regarding the heterogeneity of definitions, duplication of requests, difficulty in data reuse, and the high cost of reporting preparation are documented both in the works of the Bank for International Settlements and in documents of the FCA, FinCEN, NCA, and Reports of Council of Europe Committees, such as MONEYVAL [6–10]. That is why the modern trajectory of supervisory development is shifting from the logic of "reporting as a final product" to the logic of "data as a shared resource" suitable for reuse, automated verification, and analytical enrichment [7–9]. Despite a significant body of work on RegTech, digital transformation in the AML field, and machine-readable reporting, the literature has yet to sufficiently address the integrated architecture of an interagency system that combines granular regulatory information, state and international registries, unstructured external sources, early warning mechanisms, and analytical visualization tools within a single environment. The identified gap is decisive for constructing a modern IS RegTech for AML supervision.

The purpose of the study is to provide a scientific substantiation of the concept and architecture of IS RegTech for AML supervision, i.e., monitoring reporting entities for the needs of risk-based supervision. The working hypothesis posits that the combination of granular reporting, shared data models, and analytics of structured and unstructured sources within a single digital loop enhances the timeliness, completeness, and analytical depth of supervisory decisions.

2. Literature Review

The formation of the modern discourse on RegTech began with works in which this category was defined as the use of innovative technologies by regulatory authorities to support supervisory activities [1]. Further development of the topic led to an expansion of the interpretation: di Castri et al. [3] proposed considering RegTech not only as individual digital tools but also as an evolution of supervisory technology generations – from manual and descriptive processes to big data, artificial intelligence, and automated decision-making. More recent empirical evaluations indicate that the successful implementation of RegTech depends both on the availability of algorithms and on institutional factors, including an overall digital transformation strategy, data governance policy [12].

A separate body of literature is dedicated specifically to the application of supervisory technologies in the field of AML. Coelho, De Simoni, and Prenio [2] show that authorities responsible for AML supervision and financial intelligence are increasingly using network analysis, text mining, NLP, and machine learning to integrate large volumes of structured and unstructured data. The FATF and the Egmont Group emphasize that digital transformation in this area is a response to three basic challenges: processing speed, information volume, and the variety of data formats [4]. At the same time, the FATF [5] highlights the second dimension of the problem – confidentiality, data protection, the legal frameworks for information sharing, and the explainability of analytical tools. Another important line of research concerns the modernization of regulatory reporting. Crisanto et al. [7] substantiate the transition from traditional report submission to a data-sharing model, in which supervisory authorities work with data as a reusable asset. The FCA in the Digital Regulatory Reporting project [6] and the Bank of England in the Transforming Data Collection program [8] demonstrate the potential of machine-readable and machine-executable instructions, shared data dictionaries, and attribute unification. A logical continuation of this paradigm was Project Ellipse, which showed that the combination of granular reporting, a shared cross-border data model, and external unstructured sources can provide supervision close to real-time [9]. The arguments in favor of such a transformation are reinforced by EBA data: the complexity of regulatory requirements, the volume

of reporting obligations, and internal data preparation operations are among the most significant drivers of reporting costs [10]. Despite the intensive development of this topic, most existing works either describe general RegTech taxonomies, analyze individual pilot solutions, or focus on sectoral reporting requirements. Significantly less attention is paid to constructing a comprehensive interagency architecture for AML supervision that would simultaneously address the unification of data descriptions, the consolidation of a supervised entity's profile from multiple registries, the analytics of market, sanctions, and reputational signals, network risk mapping, as well as early warning tools.

3. Research methodology and structure

The study is of a conceptual and applied nature. The object of the study is the process of regulatory and supervisory control in the AML field over reporting entities, while the subject consists of the methods, tools, and architectural solutions required to build the IS RegTech as an integrated digital platform. The methodological framework of the research is based on a systems approach, functional decomposition of the supervisory process, comparative analysis of international RegTech practices, conceptual data modeling, and architectural design. The logic of the research includes four sequential stages. In the first stage, the key problems of the supervisory cycle are formalized: the templated and aggregated nature of reporting, semantic inconsistency of data, time lags between information submission and utilization, as well as the fragmentation of sources. In the second stage, the specified problems are transformed into functional requirements for the IS. In the third stage, a two-level architectural model is formed, combining granular data and a shared data model with near real-time analytics. In the fourth stage, a system of performance evaluation indicators is derived, enabling a transition from a declarative description of benefits to measurable results.

In the structural dimension, the proposed system encompasses several interconnected layers. The first layer consists of data sources, which include regulatory reporting, state registries, judicial and sanctions datasets, international corporate and ultimate beneficial owner databases, as well as external unstructured sources such as news and analytical reports. The second layer is the normalization and validation loop, where a shared data model, attribute mapping, record cleansing, and reconciliation of legal entity names are implemented. The third layer is the core for storing and enriching the profiles of supervised entities. The fourth layer is the analytical loop, which includes risk scoring, network analysis, NLP text processing, anomaly detection, and the generation of early warnings. The fifth layer comprises user interfaces, monitoring dashboards, interagency exchange, and the decision audit log.

4. Results

In the modern context of the financial sector's digital transformation, the AML supervision system must operate proactively. For this reason, it is appropriate to consider IS RegTech for AML supervision as a tool for the application of innovative technologies by financial authorities to support supervisory activities. In international discourse, RegTech is primarily associated with the use of big data, analytics, artificial intelligence, and automated tools to enhance the capacity of state authorities to conduct risk-based supervision.

The relevance of implementing IS RegTech is driven by a combination of regulatory, technological, and institutional factors. First, the AML supervision and control system must keep pace with the rate of technological change and simultaneously respond adaptively to new risks generated by digital financial services, cross-border transactions, and new behavioral models of market participants. Second, there is a need to abandon ambiguous, static, and low-efficiency regulatory frameworks that fail to provide sufficient flexibility in the face of rapid changes. Third, supervisory authorities and reporting entities require a more agile regulatory environment amidst social, economic, and political upheavals. Fourth, the provided concept places special emphasis on the positive correlation between the quality of regulation, supervision, and economic development, which is visualized in Fig. 1. For

academic rigor, it is appropriate to link this argument with the Regulatory Quality indicator of the Worldwide Governance Indicators system, which the World Bank defines as the perception of the state's capacity to formulate and implement sound regulatory policies.

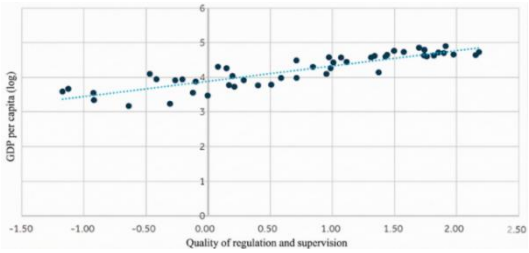

Figure 1: Positive correlation between the quality of governance and GDP per capita [Worldwide Governance Indicators (World Bank), Accenture]

Based on the presented concept, it is appropriate to group the drivers of IS RegTech implementation into four interconnected blocks. The first block consists of regulatory drivers: the growing complexity of AML requirements, the need for rapid rule updates, and improving the quality of supervisory decisions. The second block encompasses technological drivers – the accumulation of large datasets, the development of machine-readable formats, API interactions, cloud services, and advanced analytics tools. The third block is formed by organizational drivers related to the need for interagency coordination, the elimination of duplication, and the construction of a shared information space. The fourth block comprises analytical drivers, namely the need for early warning, risk scoring, the detection of hidden connections, and the prioritization of supervisory measures. This specific logic aligns with the international vision of RegTech as a combination of data collection, data processing, and data analytics for the needs of supervisory authorities.

The circle of IS RegTech participants is of an ecosystem nature. The key supervisory authorities serving as the primary users of the platform include the Ministry of Finance of Ukraine, the Ministry of Justice of Ukraine, the Ministry of Digital Transformation of Ukraine, the National Securities and Stock Market Commission, the National Bank of Ukraine, and the State Financial Monitoring Service of Ukraine.

4.1. The architecture of the IS RegTech for risk-based supervision

In the baseline concept, IS RegTech for AML supervision is defined as a digital service platform based on big data, artificial intelligence, and, if necessary, distributed ledger technologies, designed to create an autonomous, reliable, professional, and transparent mechanism of interaction between supervisory authorities and other state institutions that are participants in the AML system. Functionally, such a platform must support comprehensive verification, information disclosure, risk assessment, and dynamic monitoring of the activities of supervised entities. The general architecture diagram of IS RegTech for AML supervision is presented in Fig. 2.

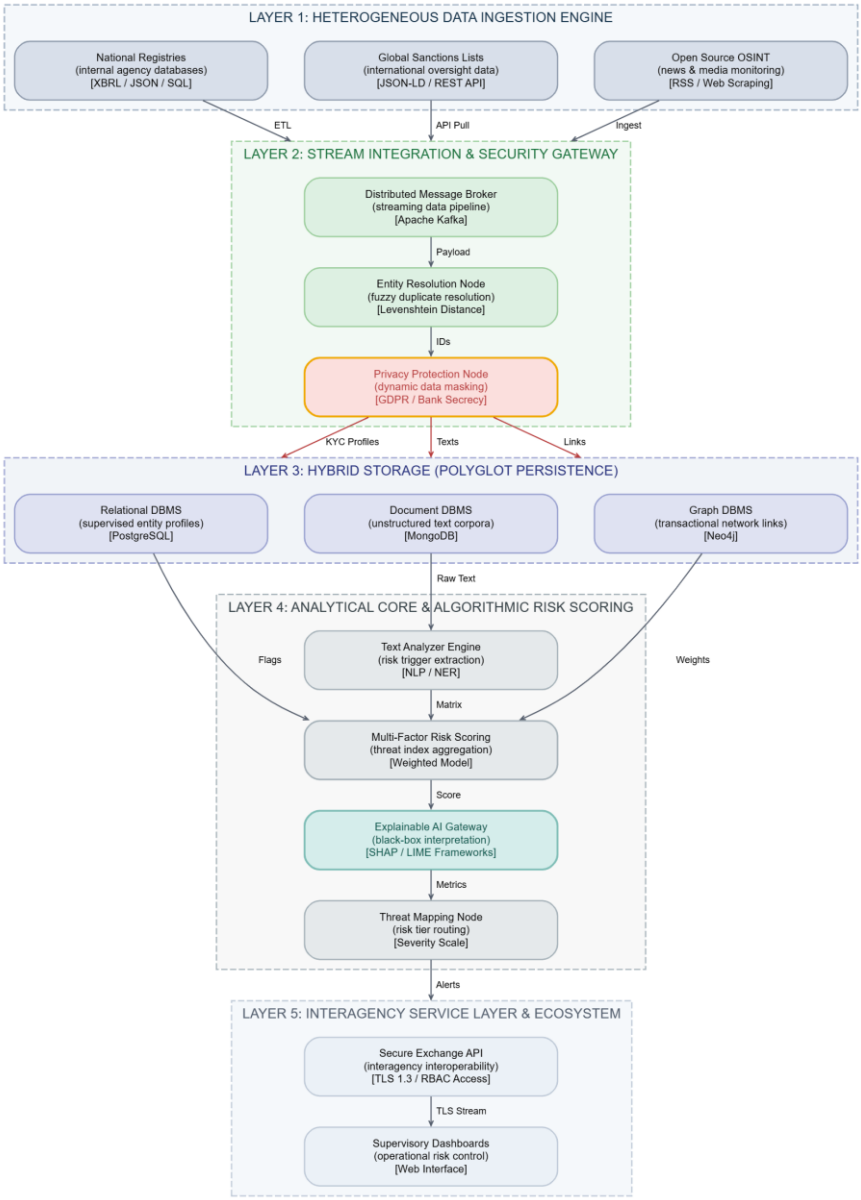

Figure 2: Architecture of the IS RegTech for AML supervision

As demonstrated in Fig. 2, the functional and technological interaction within the IS RegTech platform is organized into five specialized, sequential layers, bound by strict data-flow pipelines and interoperability standards:

Layer 1 (Heterogeneous Data Ingestion Engine): operates as the primary intake node, capturing granular structured reporting from national registries (in unified XBRL, JSON, and SQL formats), international restrictive watchlists (via automated JSON-LD and REST API pulls), and unstructured OSINT text streams using automated web-scraping and RSS feeds.

Layer 2 (Stream Integration & Security Gateway): serves as the real-time processing and compliance backbone. Heterogeneous data payloads are ingested into a distributed message broker (Apache Kafka pipeline). The system immediately routes data through a Name Unification Node (utilizing fuzzy string matching based on Levenshtein Distance) to resolve duplicates. To ensure absolute compliance with national personal data protection acts, GDPR, and bank secrecy laws, all unified profiles pass through a dedicated Privacy Protection Node where dynamic data masking and depersonalization are executed before any data reaches the analytical or storage environments.

Layer 3 (Hybrid Storage / Polyglot Persistence): addresses data variety by deploying a polyglot persistence model. Fully structured entity profiles and supervisor decision logs are maintained in a relational DBMS (PostgreSQL). Concurrent transactional linkages, complex corporate ownership

structures, and hidden cross-sectoral networks are fed into a graph DBMS (Neo4j) optimized for link analysis. Raw, unstructured textual inputs from media monitoring are channeled into a document-oriented NoSQL DBMS (MongoDB).

Layer 4 (Analytical Core & Algorithmic Risk Scoring): executes advanced threat modeling. Unstructured textual corpora are processed by a Text Analyzer Engine using Natural Language Processing (NLP) and Named Entity Recognition (NER) to isolate threat triggers and compile a sentiment scoring matrix. The Multi-Factor Risk Scoring engine aggregates these matrices with relational registry flags and graph network link weights to compute the integral risk index (TotalRisk). To completely eliminate the risk of algorithmic bias and satisfy FATF guidelines regarding the transparency of automated financial intelligence, the platform routes all black-box machine learning scores through an Explainable AI (XAI) Gateway. Utilizing SHAP and LIME frameworks, it decomposes the risk-score into clear, fact-based feature weights before passing the telemetry to the Threat Mapping Node for color-coded severity routing.

Layer 5 (Interagency Service Layer & Ecosystem Endpoints): governs secure, interoperable distribution. Prioritized risk alerts and diagnostic audit logs are transmitted to ecosystem endpoints—including the National Bank of Ukraine, the State Financial Monitoring Service, and the Ministry of Justice–via a Secure Exchange API gateway protected by TLS 1.3 encryption and a strict Role-Based Access Control (RBAC) model, enabling instantaneous, distributed supervisory monitoring.

This architecture ensures that the system transitions from a descriptive approach to an end-to-end data pipeline, where technical interaction rules, database selection, and compliance frameworks are natively integrated into the data flow. In terms of content, such an architecture implies that the IS RegTech must function simultaneously as an integration, analytical, and coordination infrastructure. The integration function consists in consolidating multiple sources into a single data loop; the analytical function lies in constructing risk indicators, anomaly detection rules, and an early warning system; the coordination function consists in ensuring interagency exchange, signal routing, and supporting collective supervisory response. It is precisely this triune role that makes the IS an information portal and a RegTech platform for risk-based supervision. The source base of the IS RegTech is heterogeneous. According to the presented concept, it must encompass Ukrainian state registries, judicial and law enforcement datasets, sanctions lists, beneficial ownership information, international corporate and registration databases, open sources, as well as specialized foreign resources relevant for analyzing cross-border connections, assets, sanctions, and high-risk jurisdictions. Such a broad source base is critically important for AML supervision, as it enables a transition from analyzing a single reporting document to analyzing interconnectedness, behavioral patterns, and external risk signals. The source base and data feed sources of the IS RegTech are presented in Table 1.

Thus, the source base of the IS RegTech is characterized by a high level of heterogeneity, combining a wide range of Ukrainian state registries, international sanctions lists, and foreign databases on beneficial ownership. Such integration of heterogeneous sources is critically important for AML supervision, as it allows specialists to detect complex behavioral patterns, analyze cross-border connections, and promptly respond to external risk signals.

Table 1
Sources of information and data for the IS RegTech

No.	Registry Name
	Registries of Ukraine
1.	Unified State Register of Legal Entities, Physical Persons–Entrepreneurs and Public Formations
2.	Unified State Register of Enterprises and Organizations of Ukraine / State Statistics Service
3.	Unified Register of Public Formations / Ministry of Justice

4. State Register of Civil Status Acts of Citizens / Ministry of Justice
5. Data from Unified and State Registers created in accordance with the legislation of Ukraine
6. State Register of Property Rights to Real Estate / Ministry of Justice
7. Unified State Demographic Register / State Migration Service
8. Registers and lists / Information on a business entity's right to provide services relating to the organisation and conduct of gambling / Unified Register of State Lotteries Established in Ukraine
9. Register of Auditors and Audit Entities / OSNAD (Audit Public Oversight Body)
10. State Register of Physical Persons – Taxpayers / STS (State Tax Service)
11. Information on the status of court case considerations / Judiciary of Ukraine
12. Register of Court Decisions / Judiciary of Ukraine
13. Database of invalid, stolen, or lost identity documents / State Migration Service of Ukraine
14. Information on stolen/lost/invalid passports of a citizen of Ukraine / verification of the legitimacy of a criminal record certificate.
15. Persons hiding from the authorities. The dataset contains information regarding persons hiding from the authorities. The information in the dataset is divided into separate resources, each corresponding to the information specified for it. Ministry of Internal Affairs of
16. Unified Register of Pre-trial Investigations / Prosecutor's Office
17. Unified State Register of Persons Who Committed Corruption or Corruption-Related Offenses
18. Registration data regarding legal entities of Ukraine
19. "Myrotvorets" website. Center for Research of Signs of Crimes against the National Security of Ukraine, Peace, Human Security, and International Law and Order.
20. Search for persons accused of committing crimes against the foundations of national security
21. NSDC Sanctions
22. "Main" criminal case regarding the full-scale invasion of the Russian Federation into Ukraine.
23. List of terrorists. List of persons related to conducting terrorist activities or against whom international sanctions have been applied
24. "War and Sanctions" portal. The portal was created by the National Agency on Corruption Prevention and the Ministry of Foreign Affairs of Ukraine.
25. Register of traitors. Database of Ukrainian state traitors: politicians, media figures, lawyers, and law enforcement officers.
26. Register of Russian war criminals.

International Registries

Sanctions

1. Consolidated United Nations Security Council Sanctions List.
2. RuAssets is a new international tool for verifying connections with public figures and individuals on sanctions lists in the CIS countries.
3. Financial sanctions imposed by the United Kingdom, specifically regarding the RF and RB.
4. State Sponsors of Terrorism list / US Department of State
5. OpenSanctions is an international database of individuals and companies with political, criminal, or economic interests.
6. Sanction List Monitor SWIFT

Foreign Companies

1. OpenOwnership is a public technology initiative that expands access to beneficial ownership information.
2. Organized Crime and Corruption Reporting Project (OCCRP).
3. Dato Capital. An online database of companies and their directors.
4. VesselFinder. Open-source tracking and information
5. Offshore Leaks Database.
6. European Union Open Data Portal. Access to open data published by EU institutions and bodies.
7. Global archive of research material for investigations.
8. Data on companies of the British Virgin Islands
9. Interactive map and database of owners of foreign companies
10. Consolidated register of insolvent companies from EU countries.
11. Official list of business registers of EU countries.
12. Official list of land registers of EU countries.
13. Register of EU countries (including Iceland, Liechtenstein, Norway).
14. Register and financial reporting data of companies from Austria. Contains paid content.
15. Risk management and compliance solutions. A resource for verifying ownership structure.

4.2. Supervisory challenges to be addressed by IS RegTech

The concept of IS RegTech stems from four basic limitations of the current supervisory model. The first limitation lies in the templated and aggregated nature of documents, where datasets are generated for a specific reporting template and are therefore nearly unsuitable for reuse. The second is the inconsistent data description across different information systems, registries, and sources, which

precludes rapid semantic mapping of information. The third limitation is related to the retrospective nature of reporting, where data arrives periodically and may no longer reflect current risk dynamics. The fourth is the lack of integration between sources, due to which important risk signals remain scattered across various databases, market announcements, and registries. The response to the aforementioned problems within the proposed model consists of five complementary solutions: the use of granular data, the implementation of shared data models, obtaining information in near real-time, the integration of structured and unstructured sources, and the construction of a modular data architecture. In aggregate, the presented components form the very RegTech loop that transitions supervision from a manual format of data collection and reconciliation into a format of automated data interpretation, risk detection, and decision support. The concept of IS RegTech is illustrated in Fig. 3.

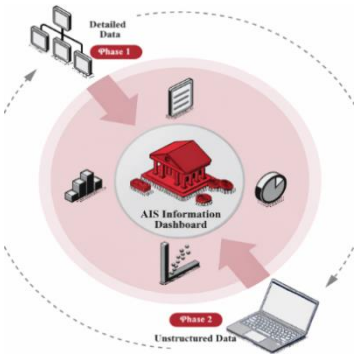

Figure 3: A framework for addressing anti-money laundering supervisory challenges using AI-based RegTech solutions

The proposed concept is implemented in two phases. Phase 1 is of an exploratory nature and involves increasing the availability of granular data through shared data models. At this stage, it is evaluated how supervisory authorities and other participants in the AML system can operate with standardized, machine-readable, and mutually consistent datasets without immediately disrupting the existing regulatory frameworks. Particular emphasis is placed on the possibility of using the same data model across different authorities and, prospectively, different jurisdictions. This approach aligns with the international trajectory of RegTech development, where data standardization is a prerequisite for subsequent analytical automation. Phase 2 involves the transition to an early warning model in near real-time. At this stage, granular regulatory reporting is integrated with unstructured sources, while artificial intelligence, machine learning, and text analytics are utilized to extract risk signals, establish correlations between events and supervisory indicators, and display the results via dashboards. As a result, the IS RegTech accumulates data capable of generating prioritized signals for supervisory attention, thereby performing the core function of RegTech in risk-based supervision.

4.3. Expected benefits, outcomes and performance measurement

The advantages of the IS as a RegTech platform, reflected in Fig. 4, consist in increasing the effectiveness of regulation and supervision, early risk detection, deepening market understanding, and ensuring high scalability of the supervisory infrastructure. First, the comprehensive architecture of the IS makes it possible to automate the full cycle of supervisory and control procedures – from data collection, validation, and integration to analytics, preparation of decisions, prevention, and mitigation of risks in the AML field. Second, the use of high-quality data, risk indicators, and early warning mechanisms creates conditions for the timely detection of threats and vulnerabilities both at the level of individual supervised entities and at the sectoral level. Third, near real-time analytics provides a deeper understanding of market processes and allows supervisory authorities to make more informed and targeted decisions.

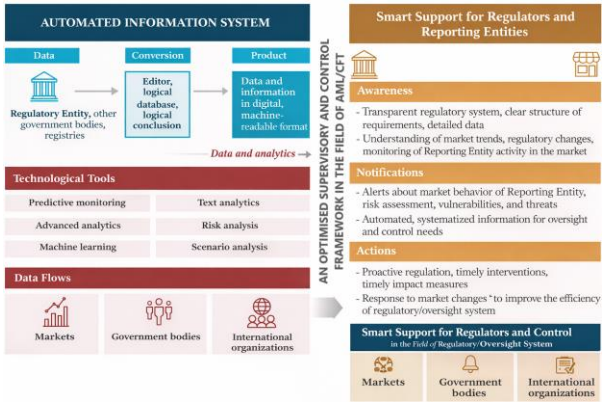

Figure 4: Key advantages of IS as a RegTech platform for risk-based supervision

Fourth, the modular construction of the IS , the use of APIs, data warehouses, and technological services ensure its scalability, i.e., the capacity to operate with growing volumes of data, regulatory requirements, and the number of system participants. The link between the conceptual advantages of the system and the tools for its implementation can be traced through the transformation of the technology stack into specific supervisory capabilities. Thus, the implementation of the specified set of technological solutions allows for a shift in the regulatory paradigm from retrospective recording of violations to proactive real-time risk management.

4.4. IS RegTech functional modules

4.4.1. Module 1. Name Unification and Identification of Supervised Entities

Bringing the names of reporting entities into a unified format enables the tracking of vulnerabilities at the systemic level regarding one and the same entity (Fig. 5).

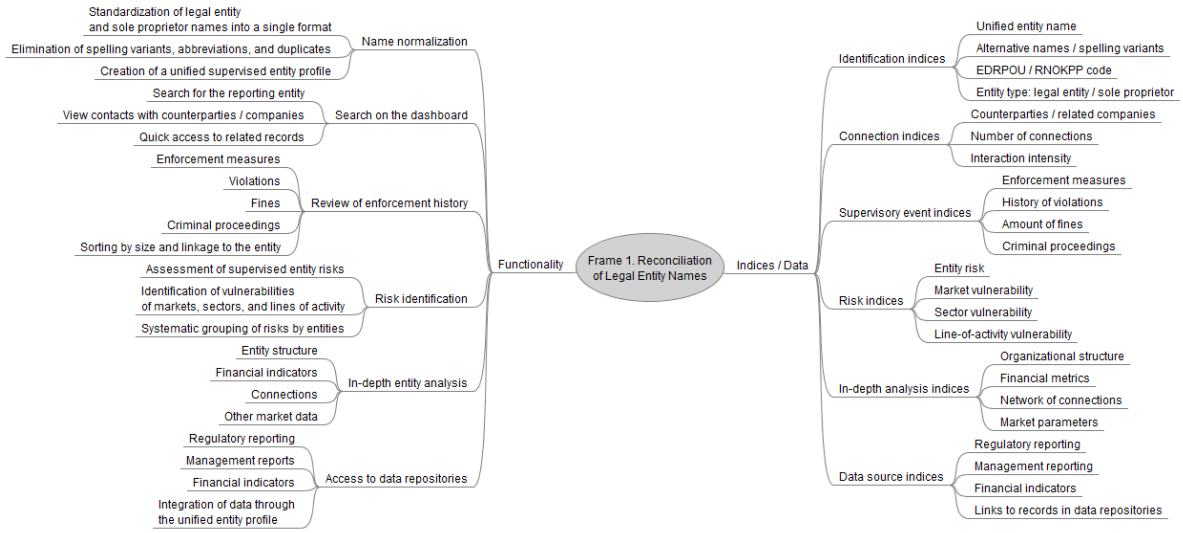

Figure 5: Conceptual diagram of the name unification and identification of supervised entities module in IS RegTech

The name unification module provides supervisory authorities with the following capabilities: search for a reporting entity using the search function on the dashboard to see its interactions with various counterparties/companies; review enforcement measures, history of violations, fines, criminal proceedings, etc., ordered by magnitude and linked to the respective supervised entity; identify risks of supervised entities. This will enable determining the vulnerability of individual markets, sectors, and fields of activity; conduct an in-depth analysis to learn more information about

the reporting entity, including its structure, financial indicators, connections, and other market data.

4.4.2. Module 2. Market and Financial Analysis

Real-time notifications based on the processing of news, market information, records, and data from various registries enable supervisory authorities to promptly investigate relevant signals or use them as a baseline for conducting more detailed analysis. The integration of regulatory datasets and unstructured sources allows to: display any current events related to supervised entities via top news alerts upon logging into the dashboard; receive early warnings regarding specific entities if text analytics detects any negative changes based on market data, news, registry updates, etc.; rank early warnings or color-code them by the degree of potential adverse risk associated with the development of events relevant to the reporting entities; route early warning notifications to the appropriate supervisory authority for investigation into the entity's activities or related information, such as the sector or jurisdiction in which the entity operates; program and configure the intelligence analysis tool to provide supervisory authorities with the following information; news regarding supervised entities and their counterparties; "sentiment" analysis of the information applied to a specific text depending on the use case, such as insolvency, default, failed, late or missed payments, bankruptcy, debt, litigation, or even changes in senior management; hyperlinks provided if there is a need to conduct a more in-depth analysis. Generally, the conceptual diagram of the market and financial analysis module in IS RegTech is presented in Fig. 6.

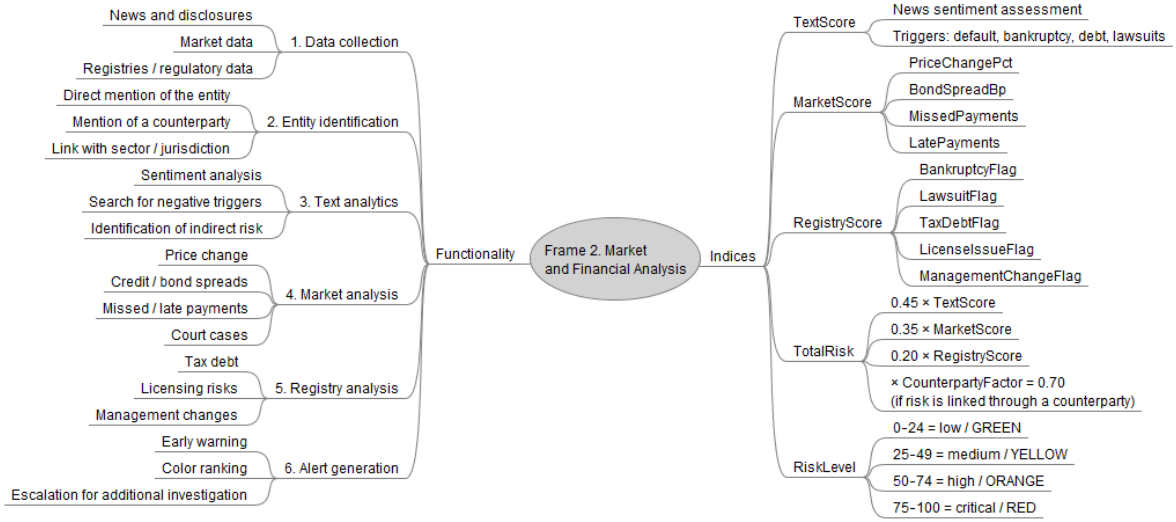

Figure 6: Conceptual diagram of the market and financial analysis module in IS RegTech

4.4.3. Mapping Vulnerabilities of Reporting Entities and Sectors to Which They Belong

Mapping the vulnerabilities of supervised entities identified as high-risk or stressed can reduce the burden on supervisory authorities, who would otherwise be forced to locate and link such information manually. Risk mapping by means of the IS opens up the following opportunities for increasing the efficiency of supervision and control: highlighting the greatest risks for supervised entities, sorted by size and corresponding type of activity; alerts regarding news, changes in the market situation, or data in registries can be tailored to select the legal entities affected by these changes, allowing supervisory authorities to investigate the notification to understand whether further actions to investigate the situation are justified; the ability to visualize the risks of reporting entities using network mapping, furthermore, supervisory authorities will be able to see cross-sectoral contagion risks; text analytics showing the sector and country in which an entity operates will allow for the identification of other legal entities operating in the same sectors and countries, which may

indicate potential supply chain risks or risks of related organizations. The conceptual diagram of the module is presented in Fig. 7.

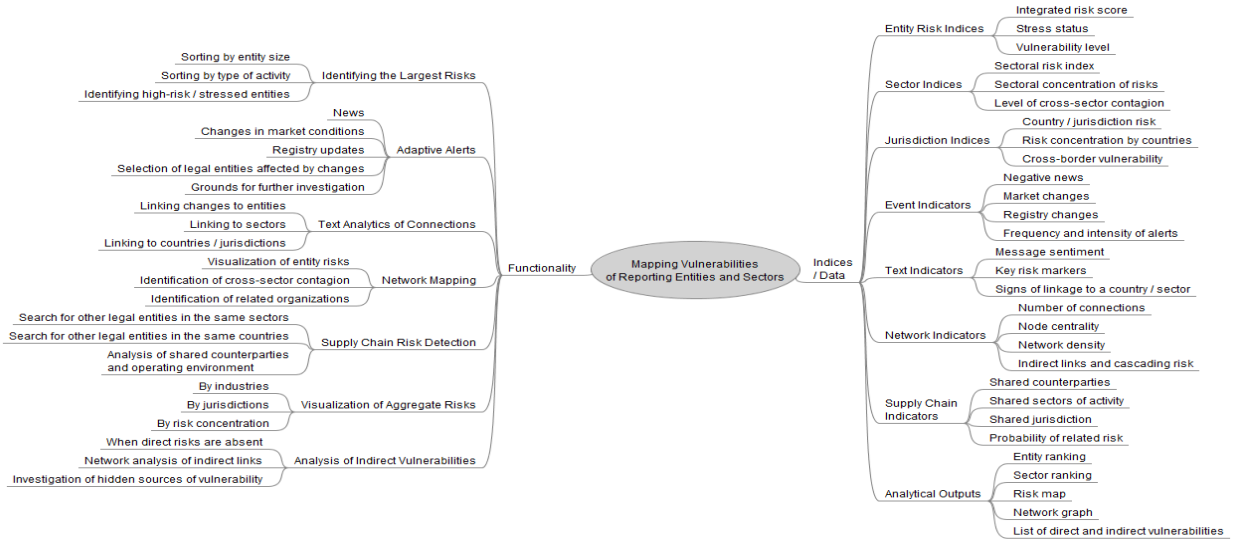

Figure 7: Conceptual diagram of the vulnerability mapping module for primary financial monitoring entities and sectors in IS RegTech

4.4.4. Module 4. Threat and Current Event Analytics

Analytical data generated on the IS RegTech platform, particularly data on risks, the current market situation, market leaders, sanctions, and violations, allows for the formation of insights into future sectoral development trends and potential scenarios (Fig. 8). The application of advanced analytics to regulatory data and current market information enables supervisory authorities to analyse how ongoing events affect AML compliance and to identify appropriate risk mitigation measures.

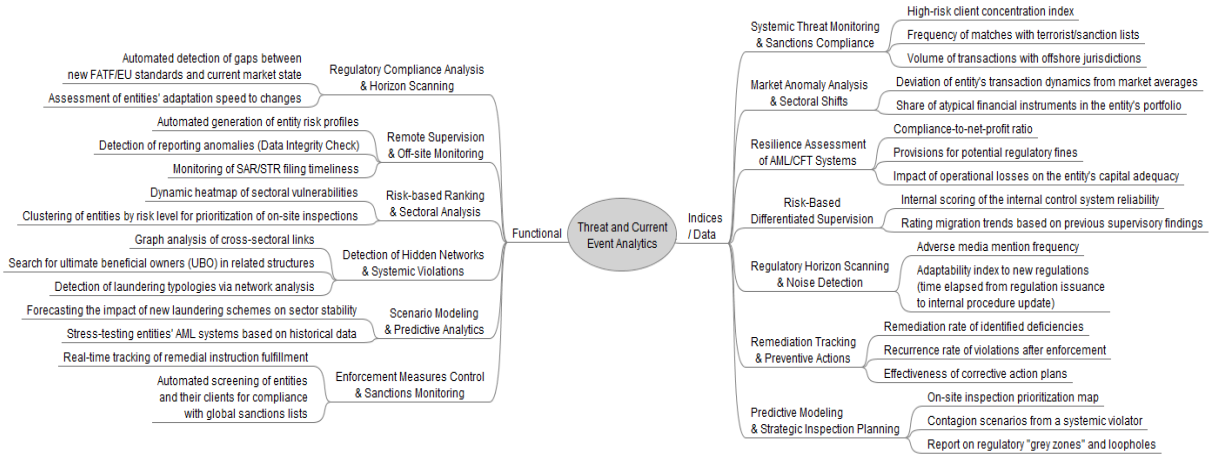

Figure 8: Conceptual diagram of the threat and current event analytics module in IS RegTech

Furthermore, this technology enables them to request financial performance metrics from supervised entities and obtain comprehensive breakdowns of the most significant risks facing major market participants.

4.5. Assessment of the effectiveness of IS in the RegTech sector

To assess the effectiveness of the IS as a RegTech platform, it is not enough to simply note the automation of individual procedures. It is necessary to measure changes across the entire supervisory cycle: from the collection, validation and processing of information to the speed of decision-making,

the quality of analytics, risk mitigation and the prevention of potential losses. At the same time, some of the effects of implementing the IS are directly quantifiable, whilst others manifest indirectly – through increased public value, market transparency, better coordination between institutions and a shift from selective to end-to-end analysis of markets and segments. Table 2 presents a systematic overview of a set of KPIs that enable a comprehensive assessment of the effectiveness of IS RegTech in the field of financial monitoring.

Table 2
Indicative performance metrics for IS RegTech

Domain / Area	Description	KPI
Efficiency enhancement in data collection and processing	Measuring the impact of automation	Transaction costs (human resources vs. technology)
Harm reduction and mitigation	Measuring public value generation	Resources saved due to anti-money laundering (AML) prevention and early warning measures
Optimization of data retrieval costs	Measuring technology adoption to eliminate duplication of efforts	Information search and reporting preparation costs
Enhancement of external stakeholder engagement	Measuring outreach and perception of initiatives among stakeholders	Evaluating the effectiveness of collaborative measures and prevention of potential market losses
Institutional modernization	Assessing institutional modernization and the elimination of interagency duplication of efforts	Budgetary allocation size; share of shared data and services
Risk mitigation	Data analytics for back-testing via feedback loops	Number of accurately predicted risks
Resource allocation efficiency	Assessing the speed of data, information, and approval acquisition	Time required for data retrieval; time required for online and offline reconciliations and clearances
Workforce productivity	Measuring the impact of automation on individual and team performance	Average number of processed cases per employee; average case processing time; share of automated operations

Therefore, the effectiveness of IS in the RegTech sector should be assessed through a multidimensional framework that combines operational, analytical, institutional and public-value indicators. The proposed KPI system shows that IS improves risk detection, accelerates decision-making, strengthens interagency coordination and reduces potential market losses. In this way, IS functions as an instrument of institutional modernization and more proactive risk-based financial monitoring.

5. Conclusion

This article proposes and theoretically validates an automated information system as a RegTech-enabled infrastructure for risk-based AML supervision, integrating multi-source data analytics to enhance regulatory transparency, early risk detection, and evidence-based supervisory decision-

making. It demonstrates that the key limitations of the traditional model are the formulaic nature of reporting, inconsistencies in data description, time lags between the submission and use of information, and the fragmentation of information sources. In response to these issues, an IS architectural model is proposed, based on granular data, common data models, the integration of structured and unstructured sources, and the use of advanced analytics for early risk warning.

The scientific novelty of the research lies in the formation of a unified conceptual framework that combines regulatory reporting, national and international registers, sanctions and market data, network and text analysis tools, as well as a KPI system for assessing the effectiveness of supervision. The practical significance lies in the fact that such a system is capable of reducing the time spent searching for and verifying information, strengthening coordination between supervisory authorities, ensuring better data quality, and enhancing the state's capacity for early risk detection.

The working hypothesis of the study has been confirmed at a conceptual level: the integration of detailed reporting, a common data model and analytics from external sources provides the basis for a more timely, comprehensive and well-founded supervisory response. Further research should focus on five areas: developing a formal common data model for reporting by supervised entities; designing secure protocols for inter-agency data exchange; empirical testing of risk-scoring algorithms and NLP models; assessing the explainability and fairness of analytical decisions; and pilot measurement of the system's KPIs in a real regulatory environment.

Prospects for further research. The potential of the IS lies in the possibility of transitioning to continuous monitoring of supervised entities' activities in near real-time, as well as the gradual expansion of the range of data sources and use cases. The accumulation of regulatory, market, sanctions, legal and international data on the platform has the potential to increase market transparency, improve the quality of AML compliance and strengthen coordination between all participants in the system. This is the strategic value of the IS as a national RegTech infrastructure.

Declaration on Generative AI

The authors declare that generative AI tools were used for limited linguistic assistance, including translation and language refinement. No generative AI tools were used to produce the scientific content, research design, data analysis, interpretation of results, or references. All substantive intellectual work was carried out by the authors, who assume full responsibility for the final version of the manuscript.

Acknowledgements

The study was conducted as part of a broader project supported by the Center for Ukrainian Research Studies at SGH (2024–2026). The DeepL service was used for machine translation and language editing of selected parts of the manuscript. All translated and edited content was reviewed, refined, and approved by the authors.

References

[1] D. Broeders and J. Prenio, Innovative technology in financial supervision (suptech): The experience of early users, FSI Insights on Policy Implementation, no. 9, Bank for International Settlements, Basel, Switzerland, Jul. 2018.

[2] R. Coelho, M. De Simoni, and J. Prenio, Suptech applications for anti-money laundering, FSI Insights on Policy Implementation, no. 18, Bank for International Settlements, Basel, Switzerland, Aug. 2019.

[3] S. di Castri, S. Hohl, A. Kulenkampff, and J. Prenio, The suptech generations, FSI Insights on Policy Implementation, no. 19, Bank for International Settlements, Basel, Switzerland, Oct. 2019.

[4] Financial Action Task Force and Egmont Group, Digital Transformation of AML/CFT for Operational Agencies: Detection of Suspicious Activities and Analysis of Financial Intelligence, Paris, France, 2021.

[5] Financial Action Task Force, Opportunities and Challenges of New Technologies for AML/CFT, Paris, France, 2021.

[6] Financial Conduct Authority, Digital Regulatory Reporting, online resource, 2023. Available: https://www.fca.org.uk/innovation/regtech/digital-regulatory-reporting

[7] J. C. Crisanto, K. Kienecker, J. Prenio, and E. Tan, From data reporting to data-sharing: How far can suptech and other innovations challenge the status quo of regulatory reporting?, FSI Insights on Policy Implementation, no. 29, Bank for International Settlements, Basel, Switzerland, Dec. 2020.

[8] Bank of England, Transforming Data Collection from the UK Financial Sector, Discussion Paper, London, U.K., Jan. 2020.

[9] Bank for International Settlements Innovation Hub, Project Ellipse: An Integrated Regulatory Data and Analytics Platform, Basel, Switzerland, Mar. 2022.

[10] European Banking Authority, Study of the Cost of Compliance with Supervisory Reporting Requirements, EBA/Rep/2021/15, Paris, France, 2021.

[11] World Bank, Worldwide Governance Indicators, online resource, 2025. Available: https://www.worldbank.org/en/publication/worldwide-governance-indicators

[12] G. Panasenko and V. Hurochkina, Intelligent Compliance as a Fundamental Tool for Ukraine's Economic Security, in: A. Semenov, I. Yepifanova, J. Kajanová (eds.), Data-Centric Business and Applications, Lecture Notes on Data Engineering and Communications Technologies, vol. 272, Springer, Cham, 2026. DOI: 10.1007/978-3-032-06608-4_1

[13] L. Gambacorta, N. Lauridsen, S. Kiuhan-Vásquez, and J. Prenio, Making suptech work: Evidence on the key drivers of adoption, BIS Working Papers, no. 1309, Bank for International Settlements, Basel, Switzerland, Nov. 2025.