DOI: 10.55643/fcaptp.3.68.2026.5184

Henriett Karolyi
PhD Student, Doctoral School of Management and Business Administration, John von Neumann University, Kecskemet, Budapest, Hungary;
ORCID: 0009-0006-1480-7245

Olena Budiakova
Candidate of Economy Sciences, Associate Professor of the Department of Smart Economics, Kyiv National University of Technologies and Design, Kyiv, Ukraine;
ORCID: 0000-0001-6028-2650

Liudmyla Akimova
D.Sc. in Public Administration, Professor of the Department of Human Resources and Entrepreneurship, National University of Water and Environmental Engineering, Rivne, Ukraine; Cyprus University of Technology, Limassol, Cyprus;
ORCID: 0000-0002-2747-2775

Kateryna Bortniak
Doctor of Legal Sciences, Associate Professor of the Department of Public Law and Humanities, V. I. Vernadsky Taurida National University, Kyiv, Ukraine;
ORCID: 0000-0002-2135-3820

Larysa Shemayeva
Candidate of Economy Sciences, Associate Professor of the Department of International Economic Relations and Business Security, Semen Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine;
ORCID: 0000-0001-9097-5191

Oleksandr Akimov
D.Sc. in Public Administration, Professor of the Department of Public Administration, Interregional Academy of Personnel Management, Kyiv, Ukraine; Scientific and Methodological Center for Personnel Policy of the Ministry of Defense of Ukraine, Kyiv, Ukraine;
e-mail: 1970aaa@ukr.net
ORCID: 0000-0002-9557-2276
(Corresponding author)

Received: 17/02/2026
Accepted: 14/06/2026
Published: 30/06/2026

FINANCIAL MONITORING IN THE BANKING SYSTEM AS A TOOL FOR ENSURING THE ECONOMIC SECURITY OF THE STATE: SYSTEMATIC REVIEW

ABSTRACT

The rapid digital transformation of the global banking sector, combined with the growing complexity of geopolitical instability, cyber threats, and cross-border financial flows, has significantly increased the strategic importance of financial monitoring systems for ensuring state economic security. Contemporary financial monitoring extends beyond its traditional compliance-oriented role and increasingly functions as an integrated mechanism of systemic risk management, financial resilience, and institutional stability. Despite extensive research on anti-money laundering (AML), counter-terrorist financing (CFT), financial technologies, and cybersecurity, existing studies remain fragmented and insufficiently integrated within a unified economic security framework. This study aims to systematize contemporary scholarly approaches to financial monitoring in the banking system and to identify the systemic relationships between financial monitoring mechanisms, technological transformation, cyber resilience, and national economic security. The research employs a systematic literature review methodology based on PRISMA principles. Academic publications, analytical reports, and institutional studies indexed in major scientific databases were analyzed using thematic synthesis and comparative analytical approaches. A total of 79 studies meeting predefined inclusion criteria were selected for in-depth analysis. The findings demonstrate that modern financial monitoring systems are evolving toward adaptive, technology-driven, and data-intensive architectures characterized by the integration of artificial intelligence, machine learning, RegTech, and predictive analytics tools. Five dominant thematic clusters were identified: technological transformation of monitoring systems; AML/CFT regulatory evolution; cyber resilience and operational security; institutional and governance mechanisms; and geopolitical determinants of financial stability. The analysis reveals several systemic contradictions shaping the contemporary monitoring environment, including tensions between innovation and regulation, transparency and privacy, automation and explainability, and globalization and economic sovereignty. The study contributes to the literature by developing an integrated conceptual framework that positions financial monitoring as a strategic component of state economic security architecture under conditions of digitalization and geopolitical uncertainty. The practical significance of the research lies in identifying strategic directions for improving monitoring effectiveness, strengthening cyber resilience, and enhancing coordination between public authorities, financial institutions, and international regulatory organizations.

Keywords: financial monitoring, banking system, blockchain, AML/CFT, management, innovation, economic security, FinTech, RegTech

JEL Classification: G18, G21, F52, O33

INTRODUCTION

The financial services industry is changing as a result of the digital revolution. Risk is dynamic; new threats to the financial services industry continue to have an impact on consumer protection laws and financial stability. The banking industry has changed as a result of the integration of financial technologies, and both banks and consumers now benefit. Among the changes that promote digital banking are self-serve kiosks, financial integration, and 24-hour access to banking services. Additionally, business structures

underwent a fundamental shift as a result of the digital age. Customers' lives are growing increasingly reliant on digitization since it makes financial services easier to access. Meanwhile, as new threats and weaknesses appear in the digital world, digital banking has grown more and more important.

Even while there are some instances of wrongdoing, the banking industry is still one of the most tightly regulated in the economy. Despite ongoing regulatory advances, fraud, market manipulation, and money laundering still happen. These are systemic issues rather than individual instances that threaten financial stability, negatively influence depositor confidence, and have sound economic repercussions (Gowin et al., 2020; Pereira et al., 2019).

Monitoring within the banking industry is critical for national economic security because it combines proactive supervision, risk assessment, and monitoring to ensure financial stability, prevent illegal actions, and defend against systemic risks. Key efforts include automated bank screening, frequent financial health evaluations, and monitoring systemic risks such as cyber threats and geopolitical conflict. This holistic approach promotes financial system integrity while also supporting a country's economic stability, ability to offer credit and payments, and overall national security.

Traditional banking laws were created for physical institutions; thus, they are unable to keep up with the quick rise of digital financial services in terms of hazards. However, there are comparable dangers for both traditional and digital banks. Respondent regulations are therefore necessary for the shift to digital banking. When creating laws for digital banking as part of the financial services sector policy, it is important to keep in mind the two policy issues of attempting to safeguard the interests of clients and the safety of the financial system. Leveraging new opportunities and addressing related issues in the new digital ecosystem is another prerequisite.

Distributed ledger technologies (DLT)-based applications like digital assets, mobile banking, FinTech platforms, and artificial intelligence (AI) expanded access to financing and improved efficiency. They also expanded the possible range of cyberthreats at the same time. Financial institutions, market infrastructures, and non-bank intermediaries are more vulnerable to sophisticated cyberattacks and operational disruptions due to their increased reliance on complex IT architectures, cloud services, and cross-border data flows.

The environment of cyber risk has also taken on a strategic component as a result of heightened geopolitical tensions. Cyber operations can be used by both state and non-state actors to undermine market confidence, interfere with the application of sanctions, or interfere with payment systems, in addition to generating financial benefit. Critical financial infrastructures, digital asset platforms, and important nodes in global value chains are increasingly impacted by incidents, which increase systemic vulnerabilities and further conflate cybersecurity, financial stability, and national security.

This unprecedentedly complex landscape of emerging threats, naturally, requires a deep comprehension of implications to nation-states' economic security, as well as appropriate shifts in regulatory and monitoring systems.

LITERATURE REVIEW

Traditional financial institutions have always been at the forefront of information technology use (Windasari et al. 2022). Nonetheless, the world of today is characterized by quick technical advancements that enable an open atmosphere. According to Dissanayake et al. (2023), the financial services industry is undergoing a dramatic change, as seen by the emergence of cutting-edge financial technology solutions that threaten traditional banking offerings. For example, the merging of the digital and physical environments has led to the emergence of new methods of client interaction (Tanda & Schena, 2019).

A critical analysis of the reviewed literature makes it possible to distinguish several dominant thematic clusters that characterize the current stage of research development in the field of financial monitoring and economic security. First, a technological cluster focuses on the digital transformation of banking systems and the emergence of FinTech and RegTech solutions (Windasari et al., 2022; Dissanayake et al., 2023; Tanda & Schena, 2019). These studies consistently demonstrate that technological innovation acts as both an efficiency-enhancing mechanism and a source of systemic vulnerability. Second, an institutional-regulatory cluster highlights the role of regulatory authorities in reducing information asymmetry and stabilizing financial markets (Nygaard and Silkoset, 2023; Iyelolu et al., 2024; Bisetti, 2024). Within this group, the regulator is conceptualized as a central coordinating agent that mitigates excessive risk-taking behaviour. Third, a security-oriented cluster integrates financial monitoring with national economic security considerations (Slawotsky, 2020; Zagorsky et al., 2023), emphasizing the growing interdependence between technological sovereignty, financial resilience, and geopolitical risks.

ISSN: 2306-4994 | eISSN: 2310-8770 | Том 3 (68), 2026

An intermediary market entity called a counteracting institution reduces the knowledge asymmetry among economic participants (Nygaard and Silkoset 2023). By controlling the financial services industry, the regulator in this study fulfills the function of lessening information asymmetry. Fintechs, banks, large tech companies, and service providers are all competitive in this developing market since they target the same clients with various information sets. Since failure can lead to excessive risk-taking behaviors, regulations are intentionally designed to rectify market defects (Iyelolu et al., 2024). As a result, having a regulator helps to increase the availability of information.

According to this theory, economic agents function in a setting where information is partial and biased. The availability of information affects how economic actors behave. In order to achieve financial advantage, decisions are made using this collection of incomplete knowledge. The idea thus provides insights into the current operating environment, where traditional banks are slowly responding and adapting due to legacy systems, while fintechs have discovered opportunities within the banking sector. However, fintechs that have improved methods for gathering data provide a way to change the banking industry.

Agency theory contends that supervisors' audits can lower shareholder monitoring costs, notwithstanding the general consensus that financial supervision is expensive for bank shareholders (Bisetti, 2024). However, the problem of economic security is perhaps more important. Developing, managing, and utilizing technological innovation, as well as maintaining domestic financial stability and core economic strength, will become more closely linked to defending national security (Slawotsky, 2020; Zagorsky et al., 2023).

At the same time, country risk, which includes political, economic, and financial concerns, has an impact on the global banking sector's stability. Studies show that reducing a nation-state's sensitivity to various economic, financial, and political risks contributes to increased banking sector stability (Athari et al., 2023). Furthermore, lowering country risk leads to greater banking sector stability in countries of both low- and high-risk. Such trends reinforce the concept that the regulatory environment in the banking industry is complicated and multi-layered, with a close connection to national security considerations.

A cross-comparison of these studies reveals several stable research patterns. First, there is a clear trend toward increasing integration between financial monitoring mechanisms and national security frameworks. Second, the literature consistently indicates a transition from rule-based monitoring models toward adaptive and data-driven approaches, including machine learning and predictive analytics. Third, the complexity of financial ecosystems has resulted in a shift from isolated institutional analysis to system-wide risk assessment and models. These patterns indicate that modern financial monitoring systems are no longer viewed as purely compliance-oriented instruments but as strategic components of national economic security architectures.

Demirguc-Kunt and Detragiache (2000) investigated the application of a multivariate logit model of the likelihood of a financial crisis to track the fragility of the banking sector at the start of the new millennium. The fragility evaluation has a clear interpretation based on in-sample statistics, and the suggested method is based on easily accessible data. The authors present a comparison of event-based and statistical approaches for identifying instances of financial crises and high banking fragility. Their findings indicate that the monthly Banking Sector Fragility Index (BSF) presented in this study is extremely useful in monitoring and identifying banking sector issues using monthly data. Because the BSF index more accurately and timely reflects changes in the sectoral climate, it considerably minimizes the probability of misidentifying crises or high fragility periods, as opposed to event-based identification methodologies. The BSF index offers the opportunity to deal with higher frequency data on banking crises. Its information content is really high.

Hilbers et al. (2013) discuss an intriguing topic in the De Nederlandsche Bank Working Paper. According to the authors, financial supervisors are under growing pressure to prove the efficacy of their operations. However, this is difficult to demonstrate in practice because it is hard to establish a causal relationship between observed outcomes and supervisory actions. In this study, we outline four lessons that financial supervisors might use to assess the consequences of their actions. Additionally, the authors offer recommendations for the creation of certain performance metrics to gauge the efficacy of financial oversight.

Antwi et al. (2023) explored the nonlinearities in the relationship between financial sector development (FSD) and anti-money laundering (AML) policies in Africa. 51 African nations' panel data from the Basel Institute on Governance, the IMF, and the World Bank's indicators were used between 2012 and 2019. The dynamic panel threshold regression and the two-step system GMM were used in the study to estimate the model. The data demonstrates that anti-money laundering laws have a favorable impact on the growth of the African financial sector. At a 1% significance level, the study discovered a significant negative coefficient for AML over the threshold and a significant positive coefficient for AML below the threshold.

DOI: 10.55643/fcaptp.3.68.2026.5184

This suggests that financial sector development below the threshold is favored by AML legislation; however, this relationship vanishes in African governments with strict AML regulations (Pavlovskyi et al., 2024). This implies that because of the expense of AML, excessive AML architecture may deter the growth of the financial sector in Africa. Financial institutions in Africa should make investments in technological solutions to fight criminal activities such as drug trafficking, terrorism, arms dealing, bribery, confiscation of their illicit funds, and other crime-related activities like cryptocurrency, digital payments, as well as third parties, and trafficking of proceeds.

In their study, Patil et al. (2025) stress that although AI and machine learning technologies have a great deal of promise to improve financial security, they must function within strong, unified legal frameworks to handle concerns about autonomy, privacy, and trust. The authors assert that in order to keep financial systems safe, compliant, and inclusive, it is necessary to concentrate on coordinating international regulatory initiatives and investigating ethical issues.

Turki et al. (2020) used Bahrain as a case study to demonstrate how implementing Regulatory Technology (RegTech) innovations in banks affects the efficacy of money laundering prevention. Because Bahrain has made an effort to establish itself as the Arabian Gulf's financial hub, the findings of this study provide insight into regional patterns. A survey instrument was sent to 100 Bahraini bankers with compliance experience in order to gather the study's primary data. Multivariate analysis results show that money laundering prevention effectiveness is highly statistically significantly influenced by transaction monitoring through RegTech and time and cost-saving features of RegTech. Electronic "know your customer" (KYC) technologies, however, are not very important as drivers. In addition to illuminating the effectiveness of RegTech, this study increases public awareness of the use and integration of RegTech platforms in the battle against money laundering. The results, in particular, offer significant insights about the implementation of RegTech capabilities in banks in modestly sized regional banking hubs.

Carretta et al. (2025) examined the deterrent effect of governance performance at the national level on detected bank misconduct from 2009 to 2019 using a proprietary, manually compiled database of 251 fines imposed by national and international authorities on 109 European banks. In order to better understand how consumer response is influenced by media coverage, the authors also look at how discovered bank misbehavior affects depositor behavior. The effectiveness of national governance has a deterrent impact, as demonstrated by the empirical approach based on probit and panel fixed effects. Additionally, the instrumental regressions demonstrate that depositors remove their money in response to detected bank malfeasance, and that this response is more pronounced during periods of significant news attention.

New issues in the "cyber" scene are determined by the banking sector's rapid digital transformation and its factual integration with FinTech. The creation of a legislative and regulatory framework for reducing cybercrime in the South African banking sector is examined by Akinbowale et al. (2023). This study is motivated by the idea that if financial institutions apply certain rules and laws in a comprehensive way, the rate of cyberfraud incidence may be decreased, and the struggle against cyberfraud can acquire greater sustainability (Sydorchuk et al., 2024). The integrated policy and regulatory framework development, according to the authors, can be accomplished in two stages: first, a mixed approach (surveys and non-parametric statistical tools) to understand how banks identify cyber fraud activities and whether the method is effective. In order to reduce the incidence of cyberfraud, the second stage involves developing policy and regulatory frameworks using feedback from survey results.

The four stages of the cybersecurity project put out by Akinbowale et al. (2023) are: i) cyber risk assessment; ii) strategy implementation; iii) monitoring; iv) reporting. Additionally, the following policy concerns were noted: awareness and training, collaboration at all levels, integration of the cybersecurity project into the organization's risk management procedures, and alignment of the initiative with the organization's goal. The banking institutions must first create or enhance current controls and reaction frameworks to cyber risks and guarantee the use of efficient risk management procedures pertaining to cyber fraud risk in order to successfully apply this framework. Second, with the help of new digital anti-fraud technology, cybersecurity measures must be developed or retrofitted. Thirdly, the organization's information security architecture must be compatible with the cybersecurity measures. Fourth, in order to support the efficient implementation of cybersecurity measures, businesses should take into account human capacity development in terms of employee awareness, training, and upskilling. Lastly, a coordinated multifaceted strategy that takes into account the synergy between all national, regional, and global cybersecurity players ought to be taken into consideration (Kuznyetsova et al., 2025). This is due to the fact that cyberfraud is a transnational crime, and improving the process of investigation, prosecution, information sharing, and mitigation requires collaboration from all cybersecurity players.

Bisetti (2024) focuses on a risky phenomenon: a common belief in the banking sector is that reporting to regulatory bodies has a detrimental effect on shareholder value because compliance takes resources away from lending and deposit-taking operations, lowers profits, and ultimately harms investors. Due to the unprecedented rise in financial institutions' reporting

obligations following the financial crisis, this viewpoint gained traction. Regulatory agencies around the world have been finding it difficult to balance obtaining accurate data on supervised entities with reducing their regulatory burdens.

However, as the experts correctly point out today, the global financial crisis demonstrated how shocks and vulnerabilities that originate not only in the banking industry but also in less regulated areas of the financial system can endanger financial stability. Activities that connect different system components and produce intricate webs of exposures and interdependencies can also result in vulnerabilities. As a result, the lessons learned from the crisis have emphasized how crucial it is for authorities to monitor and evaluate possible weaknesses in the global financial system, especially in the shadow banking industry, on a system-wide basis, both internationally and at the national level. This is especially crucial because the ongoing regulatory reform that is necessary to lower the risk that financial excesses will jeopardize financial system stability in the future will increase bank costs and somewhat restrict their operations, which will provide more incentives for credit-intermediation activities to shift to the shadow banking sector. Furthermore, the conflict in Ukraine has increased the likelihood of offensive cyberattacks, which might have a negative effect on regional and global financial stability. Because more transactions were made remotely as a result of the COVID-19 pandemic and Russia's war against Ukraine, scholars also point out that cybercrime has become more common. Additionally, a number of threat actors exploited these disturbances to commit cyberfraud, including phishing and spamming (de Weijer et al., 2024; Gupta et al., 2024). Therefore, it is imperative to understand new financial monitoring concepts in the banking sector that may effectively contribute to the economic security of nation-states, including from the perspective of global banking and the stability of the financial system.

Despite the significant progress achieved in the development of financial monitoring systems, the literature also demonstrates several notable contradictions. On the one hand, technological innovations such as artificial intelligence and distributed ledger technologies are widely recognized as tools for improving transparency, efficiency, and fraud detection capabilities. On the other hand, the same technologies generate new categories of systemic risk, including cyber vulnerabilities, data integrity challenges, and regulatory fragmentation across jurisdictions. Another contradiction emerges between the increasing complexity of regulatory frameworks and the operational flexibility required by financial institutions. While stricter regulation enhances stability, it simultaneously increases compliance costs and may stimulate regulatory arbitrage or migration of financial activities to less regulated sectors.

Current studies predominantly examine: AML/CFT mechanisms, FinTech innovation, cybersecurity threats, or regulatory technologies separately. However, insufficient attention has been devoted to: the systemic interdependence between financial monitoring and national economic security; the interaction between geopolitical instability and financial surveillance mechanisms; the role of AI-driven monitoring architectures in strengthening state resilience; integrated cross-sectoral frameworks combining AML, cyber resilience, and economic sovereignty. Therefore, this study addresses the gap by conducting a systematic synthesis of interdisciplinary literature and proposing an integrated conceptual framework of financial monitoring as a strategic component of economic security.

AIMS AND OBJECTIVES

The article aims to investigate the direct patterns of financial monitoring influence on the economic security of states. With this in mind, the core task of research lies in outlining state-of-the-art concerns, challenges, prospects, and systemic connections within the landscape of financial monitoring and regulation in the field of preventing money laundering and terrorist financing. Also, the research task includes an investigation of geopolitical and geoeconomic factors' role in the field of both banking/fintech risks and the regulation changes processes.

Research questions are formulated as follows:

- RQ1. How has financial monitoring evolved under digital transformation?
- RQ2. What systemic relationships exist between financial monitoring and economic security?
- RQ3. How do FinTech, RegTech, and geopolitical risks reshape AML/CFT mechanisms?
- RQ4. What contradictions limit the effectiveness of financial monitoring systems?

METHODS

This study employs a systematic literature review (SLR) methodology aimed at identifying, evaluating, and synthesizing contemporary scholarly approaches to financial monitoring in the banking sector and its role in ensuring state economic security. In contrast to traditional narrative reviews, the systematic review approach enables a transparent, reproducible,

DOI: 10.55643/fcaptp.3.68.2026.5184

and analytically structured synthesis of fragmented interdisciplinary research related to anti-money laundering (AML), counter-terrorist financing (CFT), financial technologies, cybersecurity, and economic security.

The methodological design of the study was developed in accordance with the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) principles. The review process consisted of four sequential stages: identification, screening, eligibility assessment, and final inclusion of relevant studies.

The literature search was conducted using the scientific databases Scopus, Web of Science, ScienceDirect, SpringerLink, and Google Scholar. To ensure comprehensive coverage of the research field, both academic publications and selected analytical reports issued by international financial institutions and regulatory organizations were included. The search process focused on studies published between 2015 and 2025, reflecting the period of accelerated digital transformation of financial systems and the expansion of FinTech and RegTech ecosystems.

The search strategy was based on combinations of the following keywords and Boolean operators:

$$("financial\ monitoring"\ OR\ "anti-money\ laundering"\ OR\ "AML"\ OR\ "counter-terrorist\ financing"\ OR\ "CFT")$$

$$AND$$

$$("banking\ system"\ OR\ "financial\ institutions"\ OR\ "digital\ banking")$$

$$AND$$

$$("economic\ security"\ OR\ "financial\ stability"\ OR\ "national\ security")$$

$$AND$$

$$("FinTech"\ OR\ "RegTech"\ OR\ "cybersecurity"\ OR\ "digital\ transformation")$$

The inclusion criteria were as follows:

- peer-reviewed journal articles, institutional reports, and analytical studies;
- publications in the English language;
- studies directly related to financial monitoring, AML/CFT regulation, banking supervision, RegTech, cybersecurity, or economic security;
- empirical, conceptual, or review-based studies containing substantive analytical findings;
- full-text availability.

The exclusion criteria included:

- duplicate publications;
- conference abstracts without full papers;
- studies lacking relevance to banking sector monitoring;
- (narrowly technical studies unrelated to financial security implications;
- publications without sufficient methodological or analytical transparency.

The initial database search identified 141 publications. After removing duplicates and screening titles and abstracts, 122 records were retained for preliminary assessment. Subsequently, full-text evaluation was conducted for 94 studies. Following an eligibility assessment based on the predefined criteria, 79 studies were included in the final analytical sample. The overall study selection procedure is presented in the PRISMA flow diagram (Figure 1).

The analytical stage of the review employed thematic synthesis and comparative analysis. The selected studies were coded according to their primary research focus, methodological orientation, technological dimension, and security implications. During the coding process, five dominant thematic clusters were identified: (1) technological transformation of financial monitoring systems; (2) AML/CFT regulatory mechanisms; (3) cyber resilience and operational security; (4) institutional and governance frameworks; and (5) geopolitical and geoeconomic determinants of financial stability.

In addition to thematic categorization, the study applied a systemic analytical approach aimed at identifying interconnections, contradictions, and emerging patterns across the reviewed literature. Particular attention was devoted to the interaction between technological innovation, regulatory expansion, operational adaptability, and economic sovereignty. This approach made it possible to move beyond descriptive analysis and develop an integrated conceptual interpretation of financial monitoring as a strategic instrument of state economic security.

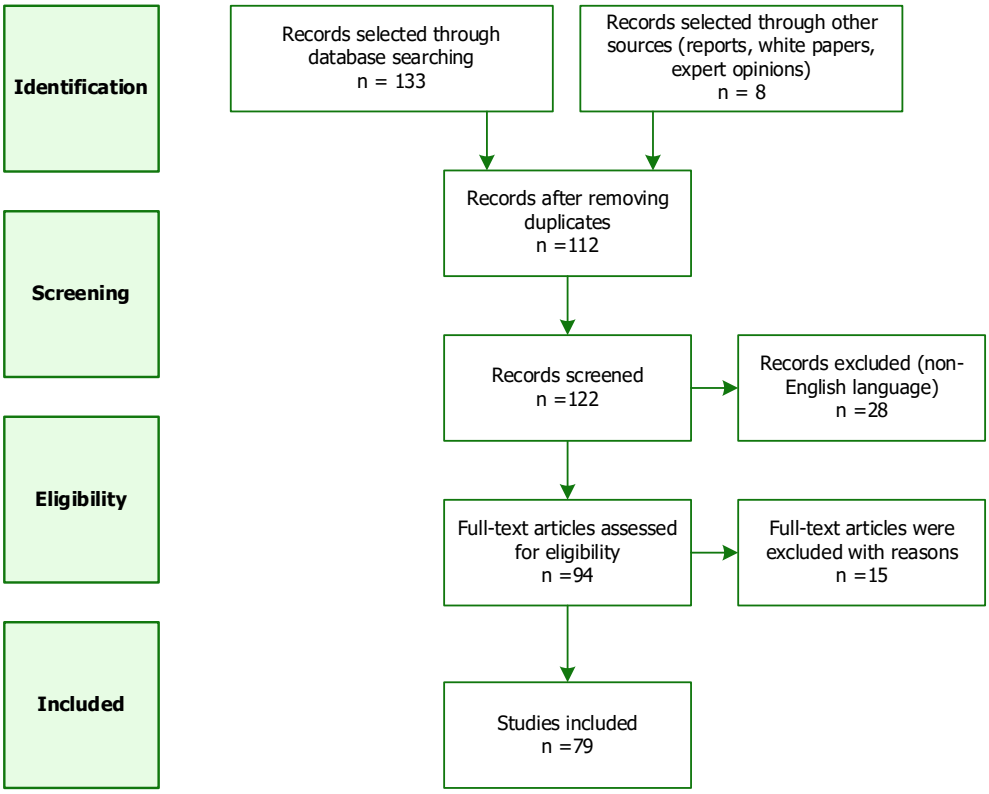

Figure 1. PRISMA flow diagram.

The theoretical foundation of the research combines elements of institutional theory, systems theory, and risk governance approaches. Institutional theory was used to examine the role of regulatory authorities and governance structures in reducing information asymmetry and stabilizing financial systems. Systems theory provided the basis for analyzing financial monitoring as a multidimensional and interconnected security mechanism operating across technological, institutional, and geopolitical domains. Risk governance perspectives enabled the interpretation of AML/CFT monitoring as part of broader national resilience and economic security architectures.

Several limitations of the study should also be acknowledged. First, the review was limited to English-language publications, which may exclude relevant regional studies. Second, the rapidly evolving nature of digital financial technologies may lead to the emergence of new regulatory practices after completion of the review process. Third, the study primarily focuses on conceptual and analytical synthesis rather than quantitative meta-analysis due to the heterogeneity of the reviewed literature. Nevertheless, the adopted methodological approach provides a sufficiently comprehensive and systematic basis for identifying the dominant trends, contradictions, and developmental trajectories of financial monitoring systems in the contemporary banking environment.

RESULTS

The systematic literature review demonstrates that financial monitoring in the banking sector has undergone substantial conceptual and technological transformation over the last decade. The reviewed studies indicate a gradual transition from traditional compliance-oriented monitoring models toward adaptive, technology-driven, and system-wide security architectures. Contemporary financial monitoring increasingly integrates artificial intelligence, machine learning, predictive analytics, cybersecurity instruments, and RegTech solutions into broader national economic security frameworks. The analysis of the selected studies revealed five dominant thematic clusters that characterize the current structure of scholarly discourse in the field of financial monitoring and economic security (Table 1).

DOI: 10.55643/fcaptp.3.68.2026.5184

Table 1. Dominant thematic clusters identified in the systematic literature review. *(Source: developed by the authors based on systematic review results)*

Thematic cluster	Core research focus	Main findings in the literature	Identified research gap
Technological transformation of financial monitoring	AI, machine learning, predictive analytics, automation of AML/CFT systems	Transition from rule-based to adaptive monitoring architectures; increasing use of AI-driven detection systems	Limited explainability and transparency of algorithmic decisions
AML/CFT regulatory evolution	Regulatory compliance, transaction monitoring, suspicious activity detection	Strengthening of international AML/CFT standards and supervisory mechanisms	Regulatory fragmentation across jurisdictions
Cyber resilience and operational security	Cybersecurity risks, digital banking vulnerabilities, and operational resilience	Growth of cyber threats targeting financial infrastructures and digital assets	Weak integration between cybersecurity and the AML framework
Institutional and governance mechanisms	Supervisory governance, regulatory coordination, public-private cooperation	Importance of institutional quality and inter-agency coordination	Insufficient system-wide governance models
Geopolitical and geoeconomic determinants	Sanctions, hybrid threats, geopolitical instability, and economic sovereignty	Increasing influence of geopolitical tensions on financial monitoring systems	Limited research on financial monitoring as a national security instrument

The findings indicate that the largest share of contemporary studies is concentrated within the technological transformation cluster. Scholars consistently emphasize the rapid integration of artificial intelligence, machine learning, and data analytics into transaction monitoring systems. The reviewed literature demonstrates that financial institutions increasingly rely on automated detection mechanisms capable of identifying suspicious transaction patterns in real time. At the same time, the literature reveals growing concerns regarding algorithmic opacity, explainability, accountability, and ethical governance of AI-driven monitoring systems.

The second major cluster concerns the evolution of AML/CFT regulation. Studies within this stream emphasize the growing complexity of international regulatory standards and the expansion of compliance obligations imposed on banking institutions. The literature demonstrates that modern AML/CFT systems increasingly rely on risk-based approaches, enhanced customer due diligence procedures, and integrated transaction monitoring infrastructures. Simultaneously, scholars identify significant tensions arising from inconsistencies between national regulatory regimes, which complicate cross-border monitoring and increase operational burdens for financial institutions.

A separate and rapidly expanding research stream focuses on cyber resilience and operational security. The reviewed studies indicate that digital transformation has significantly increased banks' exposure to cyber threats, ransomware attacks, data breaches, and operational disruptions. Financial monitoring is therefore increasingly interpreted not only as a compliance mechanism but also as an element of cyber resilience architecture. Researchers emphasize that cyber risks possess systemic characteristics capable of destabilizing financial markets and undermining public confidence in banking institutions.

The literature further demonstrates the growing importance of institutional and governance dimensions of financial monitoring. The reviewed studies consistently highlight the role of supervisory authorities, international organizations, and public-private partnerships in maintaining financial stability. Effective coordination between regulators, financial intelligence units, commercial banks, and technological providers is identified as a necessary condition for the effectiveness of modern monitoring systems. Finally, the review identifies an emerging geopolitical cluster connecting financial monitoring with state economic sovereignty and hybrid threats. Contemporary studies increasingly recognize that geopolitical instability, sanctions regimes, cyber warfare, and strategic competition between states directly influence the architecture of financial monitoring systems. Under such conditions, financial monitoring evolves into a strategic mechanism of economic resilience and national security protection.

The systematic review also revealed several recurring contradictions shaping the evolution of contemporary financial monitoring systems (Table 2).

Table 2. Systemic contradictions in contemporary financial monitoring systems. *(Source: developed by the authors based on systematic review results)*

Contradiction	Description	Implications for economic security
Innovation vs regulation	Rapid technological innovation exceeds the adaptability of regulatory frameworks	Regulatory lag increases systemic vulnerabilities
Transparency vs privacy	Expansion of monitoring mechanisms may conflict with data protection and privacy rights	Growing legal and ethical tensions
Automation vs explainability	AI-driven monitoring systems improve efficiency but reduce the interpretability of decisions	Risks of algorithmic opacity and governance failures
Globalization vs economic sovereignty	Cross-border financial integration complicates national regulatory control	Increased exposure to external systemic risks
Security vs operational flexibility	Stricter AML/CFT compliance increases operational costs and institutional rigidity	Potential reduction of banking sector efficiency

The identified contradictions demonstrate that financial monitoring systems operate within highly dynamic and multidimensional institutional environments. While technological innovation substantially improves the effectiveness of monitoring mechanisms, it simultaneously generates new categories of systemic risk requiring continuous regulatory adaptation.

The review additionally demonstrates that the evolution of financial monitoring systems follows several stable developmental trajectories. First, monitoring systems increasingly rely on predictive and data-driven approaches rather than static rule-based models. Second, cybersecurity considerations become progressively integrated into AML/CFT frameworks. Third, financial monitoring expands beyond banking supervision and gradually becomes embedded within broader state security architectures. Fourth, the interaction between public authorities and private technological actors intensifies, creating hybrid governance models in the sphere of financial security.

To further systematize the reviewed literature, the selected studies were categorized according to their methodological orientation and analytical focus (Table 3).

Table 3. Analytical characteristics of selected studies included in the review. *(Source: developed by the authors based on systematic review results)*

Research orientation	Dominant methodological approaches	Main analytical focus
Regulatory studies	Legal and institutional analysis	AML/CFT regulation and compliance
Technological studies	Case studies, computational models	AI, machine learning, RegTech
Cybersecurity studies	Risk analysis and resilience models	Operational and cyber threats
Economic security studies	Systemic and conceptual analysis	Financial stability and national security
Governance studies	Comparative institutional analysis	Supervisory coordination and policy effectiveness

The distribution of methodological approaches indicates the highly interdisciplinary nature of the field. However, the review simultaneously demonstrates fragmentation between technological, regulatory, and security-oriented research streams. Existing studies often analyze financial monitoring either from a purely technological perspective or from a narrow compliance-oriented viewpoint, while systemic interconnections between monitoring mechanisms and state economic security remain insufficiently conceptualized. Based on the conducted synthesis, the review identifies a broader transformation of financial monitoring from a narrowly specialized compliance function into an integrated mechanism of economic resilience. Contemporary monitoring systems increasingly combine technological infrastructures, institutional governance mechanisms, geopolitical risk management, and cybersecurity strategies into unified security architectures.

The systematic analysis also demonstrates that future development of financial monitoring systems will largely depend on the ability of states and financial institutions to balance technological innovation, operational efficiency, regulatory coordination, and protection of economic sovereignty under conditions of accelerating digital transformation and geopolitical instability.

In the literature, it is often claimed that banks have historically been heavily regulated and overseen due to their distinctive qualities and significance to the stability of the financial system and the actual economy (Hanson et al., 2024; Devi, 2025). The risks to the financial system (and real economy) resulting from the growing size and complexity of major banks were brought to light by the global financial crisis and the bailouts of giant, too-big-to-fail banks that followed. The goal of later regulatory changes, such as the US Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (henceforth

DOI: 10.55643/fcaptp.3.68.2026.5184

referred to as the Dodd-Frank Act), was to better regulate and oversee major banks (over a certain asset size threshold). The danger that big banks present to the financial system seems to have decreased as a result of these modifications, which brought about a period of so-called tiered bank regulation. Nonetheless, the expenses associated with banks' regulatory compliance and government organizations' control of the financial sector have risen (Hogan and Burns, 2019; Hrytsenko et al., 2020). This has prompted many stakeholders, especially lobbyists and executives at big banks, to demand that many of the post-global financial crisis regulatory reforms be loosened or eliminated. The Economic Growth, Regulatory Relief, and Consumer Protection Act (EGRRCPA) was passed by the US Congress in 2018. Many of the rules put in place after the Dodd-Frank Act were eliminated by the EGRRCPA, which led to a decrease in regulatory obligations and oversight of some big banks. However, researchers found that the risk of big banks was affected by this reduction in regulatory control (Chronopoulos et al., 2023). Chronopoulos et al. (2023) discovered that a shift in regulatory monitoring increases risk for large bank holding companies (BHCs) using a sample of BHCs from 2015Q1 to 2020Q1. Affected BHCs contribute more to the systemic risk in addition to raising the risk at the bank level. These BHCs also benefit from lower compliance costs, greater market valuation, and enhanced profitability. In the end, the authors stress that a decrease in regulatory supervision leads to a rise in bank risk. The government organizations in charge of monitoring big banks and ensuring the financial system's stability can benefit from our findings. Additionally, they show that a decrease in regulatory supervision raises the risk at the bank level.

The summarized key components of banking sector monitoring for economic security are presented in Table 4 below.

Table 4. Key components of banking sector monitoring. *(Source: Dill (2019), Lessambo (2023), Poliova et al. (2024))*

Component	Essence
Proactive Supervision	Regulatory organizations, such as the Federal Reserve, use automated technologies and on-site examinations to regularly monitor banks' financial health and performance. This enables early discovery of faltering institutions and directs supervisory attention to where it is most required.
Systemic Risk Management	Authorities monitor potential threats to the entire financial system, not just individual banks. This includes assessing risks connected with markets, major institutions, cybersecurity, and global events, as performed by the Financial Stability Oversight Council (FSOC) in the U.S.
Assessments of Financial Stability	IMF Financial Sector Assessment Program (FSAP) conducts in-depth, country-specific assessments of the financial sector's resilience and regulatory framework.
Countering Illicit Finance	Financial monitoring is crucial in preventing and countering money laundering, terrorist financing, and corruption by examining financial transactions and collaborating with law enforcement and financial intelligence units.
Data and Metrics	Monitoring utilizes a wide range of data, including a bank's capital adequacy ratios, loan quality, liquidity, and the concentration of assets within the banking system.
Public-Private Collaboration	Governmental and private sector cooperation is essential for effective monitoring in order to recognize and reduce risks, especially when it comes to matters like cybersecurity.
International Cooperation	International organizations like the IMF and the Financial Stability Board (FSB) collaborate to monitor regional and global financial stability due to the global structure of the financial system.

A range of studies describe findings indicating that vulnerabilities in data security, privacy, and regulatory compliance increased due to the increasing complexity of global financial networks and the digital transformation fueled by AI and decentralized technology (Patil et al., 2025; Wang et al., 2024; Anil & Bobatope, 2024; Adegbite, 2025). These difficulties are especially severe in the financial sector, where organizations have to adhere to many national and international regulatory frameworks in addition to protecting sensitive financial data. There are still difficulties in striking a balance between innovation and regulatory compliance across jurisdictions, despite the fact that regulatory regimes, especially in the EU, have made great strides in addressing AI-related risks in banking (Shoetan & Familoni, 2024).

To combat money laundering and terrorist funding, financial surveillance of the banking sector combines government rules with risk-based strategy implementation at the bank level. This includes implementing robust compliance systems, doing customer due diligence, monitoring for unusual activity, and reporting it to authorities such as the Financial Crimes Enforcement Network (FinCEN). Organizations such as the Financial Action Task Force (FATF) establish worldwide standards, while national agencies such as the United States Treasury and the Federal Deposit Insurance Corporation (FDIC) implement and enforce these measures through legislation such as the Bank Secrecy Act. Meanwhile, money laundering remains a threat to financial sector stability. Banks, as "gatekeepers" to the financial system, constantly combat money laundering and terrorism financing. However, as a range of scholars emphasize, AML efforts of nation-states are generally focused on domestic issues, and as a result, they frequently lag. Regulators in the banking domain also play an important role, but they frequently don't make the greatest use of limited resources, and differing approaches impede efficient worldwide collaboration. Using machine learning, the IMF, in collaboration with one of the Nordic-Baltic countries, identified flows

with potentially higher-risk countries that deserve further investigation (Ohinok & Kopylchak, 2024; Chitimira & Munedzi, 2023; AlQudah et al., 2025; Zavoli & King, 2021).

Furthermore, banks engaged in money laundering cases experience considerable decreases in equity values and greater costs for insuring against failures; related banks also suffer (Figure 2), and collectively such banks create evident risks for economic security.

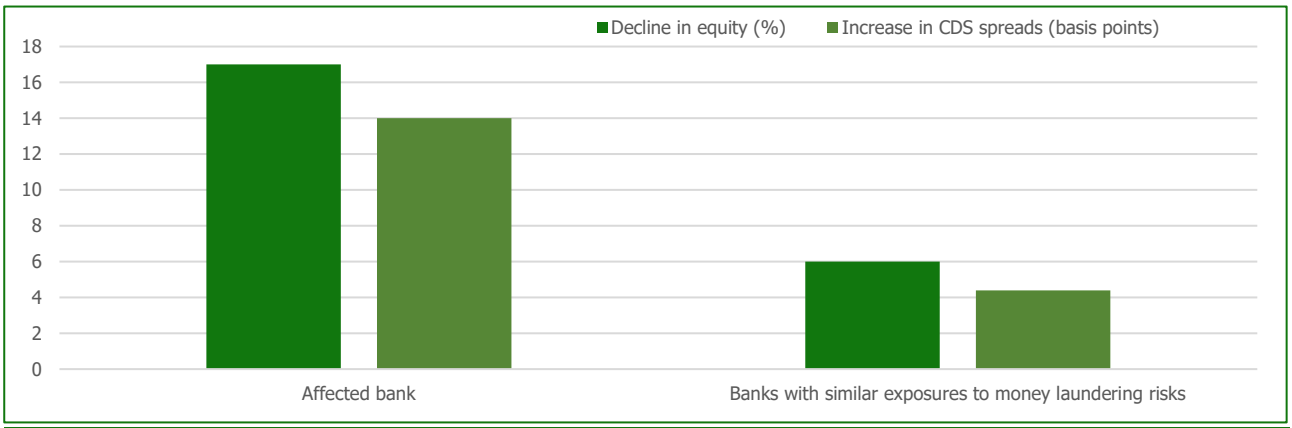

Figure 2. Shocks to stock and CDS prices during financial integrity crises (for 2022). Note: * CDS – credit default swap. *(Source: Bardin et al., 2023)*

The Fintech Transaction Monitoring Market is projected to increase at a compound annual growth rate (CAGR) of 16.97% from 2026 to 2033, from its 2025E valuation of USD 6.22 billion to USD 21.72 billion. Due to the growing number of financial fraud instances, the need to comply with regulations, and the growing usage of digital payment methods, transaction monitoring in the fintech sector is growing. Fintech businesses are investing in monitoring systems driven by AI and ML to detect suspicious activity, ensure real-time transaction analysis, and reduce financial crime (Rodríguez Valencia et al., 2025; Gelle, 2024). Furthermore, the need for sophisticated transaction monitoring systems that improve security and operational effectiveness is being driven by the growth of mobile wallets, internet banking, and cross-border payments. For real-time fraud detection and compliance across digital and cross-border payments, 82% of fintech companies employed AI-driven monitoring (Transaction Monitoring in Fintech Market Size, 2025).

In light of this, it is intriguing to examine worldwide money laundering statistics. Currently, between USD 800 billion and USD 2 trillion is laundered annually worldwide. About USD 300 billion in money will be laundered in the USA in 2025, accounting for 15% to 38% of all money laundering activity worldwide, according to KYC Hub statistics. It is anticipated that the anti-money laundering software market will grow to a size of about USD 2.56 billion worldwide. An estimated 600 money laundering cases are anticipated each year (D'Souza & Madrekar, 2025).

The USA was the largest source of laundered money in 2024, contributing USD 13,20,228 million yearly, or 46.3% of the total (D'Souza & Madrekar, 2025). Other origins (for 2024) are depicted in Figure 3 below.

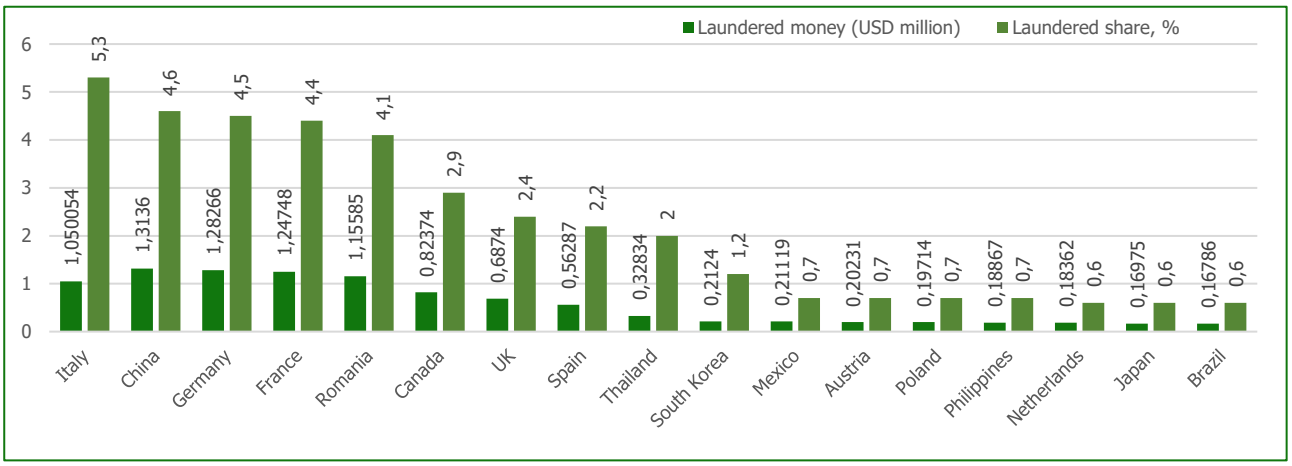

Figure 3. Top origins of laundered money statistics. *(Source: D'Souza & Madrekar, 2025)*

DOI: 10.55643/fcaptp.3.68.2026.5184

Types of anti-laundering shares statistics are presented in Figure 4.

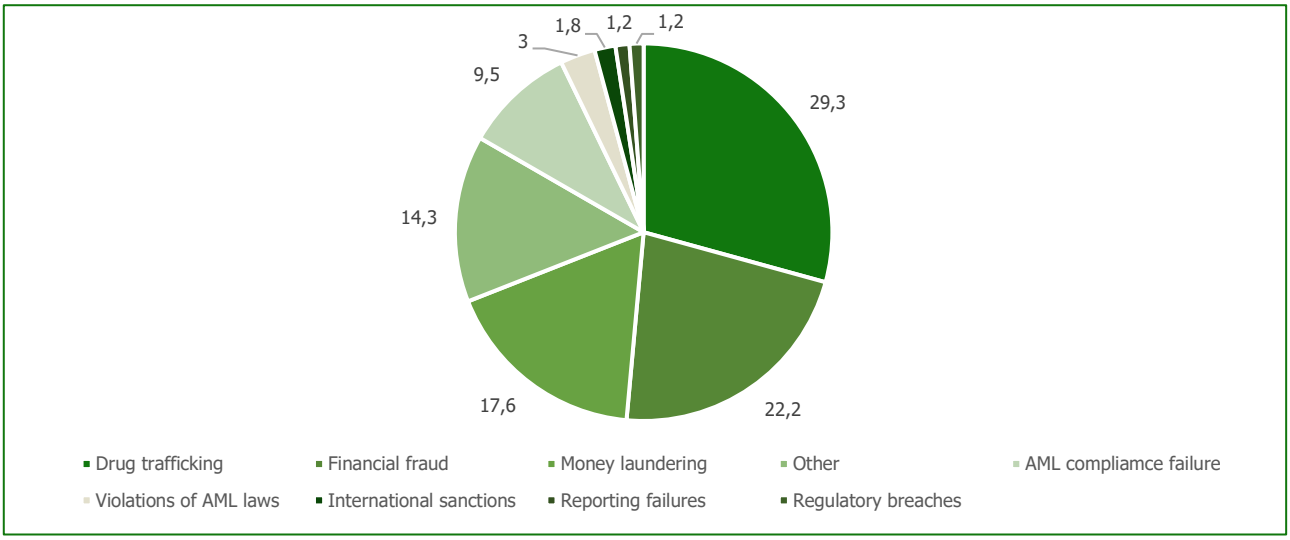

Figure 4. Types of anti-laundering shares statistics, in %, globally. *(Source: D'Souza & Madrekar, 2025)*

While the region of EU/Western Europe and North America managed to achieve some notable success in financial monitoring and anti-laundering regulation, in other regions of the world, the situation remains quite alarming (Table 5).

Table 5. Money laundering situation statistics in regions. *(Source: D'Souza & Madrekar, 2025)*

Regional Focus	Overall risk score	Quality of the AML/CFT framework	Bribery and corruption	Financial transparency and standards	Public transparency and accountability	Legal and political risk
European Union and Western Europe	3.96	4.45	3.15	3.67	2.20	2.73
Europe and Central Asia	5.16	4.99	6.08	5.13	4.05	5.82
East Asia and the Pacific	5.47	5.95	4.55	5.13	4.44	3.90
Latin America and the Caribbean	5.4	5.52	5.42	5.77	4.66	4.63
The Middle East and North Africa	5.16	4.99	6.08	5.13	4.05	5.82
North America	4.29	5.24	2.32	2.72	2.52	2.50
South Asia	5.64	5.73	5.85	5.73	4.61	5.25
Sub-Saharan Africa	6.54	6.88	6.36	6.3	5.31	5.34

United States money laundering offences statistics show a rise in the number of individuals sentenced to money laundering over time (Figure 5).

Figure 5. Number of individuals sentenced to money laundering, in dynamics, USA. *(Source: D'Souza & Madrekar, 2025)*

In the meantime, additional research exposes inefficiencies in the transaction monitoring techniques now in use, emphasizing the necessity for cutting-edge technologies like machine learning to lower false positives and operating costs (Oztas et al., 2024; Karolyi et al., 2025). In addition to cutting-edge methods like graph analysis and anomaly identification, experts stress the significance of scalability, accuracy, and regulatory compliance in creating efficient transaction monitoring systems.

The enormous volume of transactions that must be processed and the constantly changing tactics used by criminals provide financial institutions with formidable obstacles in their attempts to stop money laundering and terrorist financing. High false positive rates are produced by the conventional rules-based techniques used in banks, which result in higher expenses and inefficiencies. Because of this, there is a growing interest in artificial intelligence and machine learning to improve the accuracy and efficiency of existing methods. Moreover, novel techniques like anomaly detection and graph analysis are proposed to address the drawbacks of rule-based systems. The dynamic regulatory environment and the absence of global standards for transaction monitoring make it difficult for institutions to stay up to date and maintain compliance (Dill, 2021; Vuković et al., 2025). The research has also identified poor data quality as a problem for transaction monitoring. The efficacy of transaction monitoring techniques may be hampered by insufficient and erroneous data (de Willebois et al., 2011).

Additionally, it is challenging to adapt and successfully adopt new solutions due to the rapid pace of technology improvements, combined with banks' outdated technical systems. Because different jurisdictions have different regulatory requirements and standards, monitoring cross-border transactions has been noted as another problem (Zavoli & King, 2021). Financial institutions and regulators must work together for effective monitoring (Viritha et al., 2015).

Addressing bank misbehavior has been a top priority for authorities, legislators, and financial risk managers worldwide, who have put in place a variety of measures of a regulatory, enforcement, and preventive nature. Meanwhile, despite these efforts, the larger institutional environment determines how effective such policies are. According to institutional theory, the quality of the governance structure in which businesses function influences corporate behavior (Akiotu, 2022; Ratnawati et al., 2025). It is anticipated that stronger governance structures will enforce more efficient controls, lowering the possibility of wrongdoing. However, there are still a few empirical studies looking at the direct connection between discovered bank wrongdoing and national governance (Carretta et al., 2025).

A system with more accuracy can reduce the quantity of false positives produced, which is another prerequisite because it is a major issue. Given the growing number and complexity of transactions in financial institutions, scalability is another prerequisite for a new transaction monitoring technique to manage the growing volume of data (Royde, 2022). To guarantee that the strategy can grow with demand, a new technique should be able to scale both horizontally and vertically (Ali, 2019). For a new transaction monitoring method to be considered successful, it must be able to adapt to new forms of money laundering and terrorist financing (Pettersson Ruiz & Angelis, 2021). Adaptability is necessary to avoid reputational harm and lessen regulatory constraints (Olatinsu, 2024; Korpela, 2025; Pavlidis, 2023.

It should be noted that there are a number of important AML/CFT issues associated with the integration of banking and FinTech. These challenges are mostly caused by technology differences, regulatory complexity, and data-sharing friction. The financial services industry has changed as a result of bank-fintech collaborations, which present both new opportunities and difficulties for both established financial institutions and cutting-edge tech firms. Typically, a technology company provides cutting-edge methods to assist banks in providing regulated goods and services. A fintech company and a bank use their comparative advantages to reduce costs, boost convenience, and increase financial opportunities for customers through referral agreements, wallets powered by application programming interfaces, investing and credit products, and embedded finance integrations (Srinivas & Andal, 2023; Lysenko et al., 2024). Simultaneously, new financial monitoring issues emerge. Banks are forcing fintechs to adhere to more stringent standards as a result of the increased scrutiny. This includes mandating that their fintech partners establish more stringent AML policies and processes than would be necessary for nonbank companies (Ghash & Golder, 2026; Sultan et al., 2025). Regulators made it apparent through the current wave of enforcement proceedings that they expect banks to exercise the right that partnership agreements often grant them to examine and audit the compliance practices of their fintech partners. Fintech partners should be ready for more frequent and rigorous audits and assessments.

In Banking-as-a-Service (BaaS) agreements, the fintech is frequently given primary compliance duties for the program it manages. Usually, the program agreement contains a memorial to these commitments. A bank may occasionally become overly dependent on its fintech partner as a result of these usual arrangements. However, because fintechs and banks have essentially separate responsibilities, this raises the possibility of a mismatch and, eventually, noncompliance.

DOI: 10.55643/fcaptp.3.68.2026.5184

Regardless of the tasks they choose to assign to their fintech partners, banks in the United States, in particular, have their own separate Bank Secrecy Act (BSA)/AML compliance duties. In other words, banks cannot assign their fintech partners their BSA/AML responsibilities and hope for the best. A fintech's fulfillment of its own responsibilities does not imply that the bank has met the stricter standards set forth by the BSA. Recent regulatory scrutiny has focused on this imbalance. The BSA imposes the strictest compliance requirements on banks, including the need to maintain thorough AML programs, carry out customer due diligence, report cash transactions exceeding USD 10,000, keep an eye out for suspicious activity, and perform risk profiling (LexisNexis Editorial Staff, 2023).

In contrast, many fintechs do not have separate requirements under the BSA because they are technology suppliers rather than financial institutions. As an alternative, certain fintechs must comply with the BSA's money services business (MSB)1 regulations, which are less stringent than those of banks. Banks must adhere to stricter BSA regulations in a number of crucial areas, while MSBs must create, operate, and manage an efficient AML program. Banks must use more advanced monitoring systems, keep more thorough transaction records, and apply increased due diligence for higher-risk clients. In addition, banks must comply with the Customer Identification Program requirements of § 326 of the USA PATRIOT Act, undergo more regular and stringent regulatory exams, and expand responsibilities for correspondent banking connections and private banking accounts for non-U.S. individuals.

Today, the expert community warns that insufficient information technology infrastructure and operational capacity. A lot of nonbank fintech companies concentrate more on cutting-edge technology that boosts speed (Verdier, 2025). In order to maintain stability, lower fraud, manage data, and comply with regulations, businesses must modify their procedures. However, some businesses, particularly smaller ones, have not lived up to expectations. Dealing with the frequently quick pace of industry change is the biggest obstacle facing many fintech companies. The FSB also draws attention to the operational risks connected to inadequate governance or process management, which may cause financial services or vital IT infrastructure to be disrupted (Koosakul et al., 2024).

Another significant operational risk that can be made worse by inadequate operational controls is unexpected market events. For instance, during the GameStop stock frenzy, US fintech and online trading app Robinhood suffered from inadequate IT infrastructure and operational capacity (Verdier, 2025).

The integrity of international financial institutions is seriously threatened by the rising incidence of financial crime and money laundering, according to European experts (EY, 2025). The creation of the Anti-Money Laundering Authority (AMLA) in Frankfurt, Germany, is a crucial step in addressing these urgent problems in the European Union (EU). The establishment is an important step toward improving regulatory compliance and oversight within the EU. AMLA was created in reaction to the growing complexity of financial crime, which has developed in tandem with technological breakthroughs and the globalization of financial systems. AMLA seeks to strengthen cooperation among national authorities, provide uniform regulatory guidelines, and increase the overall efficacy of AML safeguards by centralizing AML monitoring.

The study by EY (2025) gathers insights regarding the opportunities, difficulties, and expectations around AMLA's role through qualitative interviews with a wide range of stakeholders, including banks, insurers, FinTech businesses, academic institutions, and regulatory agencies. The results show that financial institutions (FIs) generally agree that AMLA is crucial for promoting cooperation, increasing transparency, and enhancing risk management procedures.

Money laundering, cybercrime, fraud, and insider trading are all recognized as financial crimes. Criminals take advantage of new vulnerabilities brought forth by the digital transformation, which includes mobile payments and internet banking. Because of their anonymity and worldwide reach, cryptocurrencies in particular present serious difficulties for regulators. Despite a 29.5% drop from 2022, unlawful addresses still posed a significant risk in 2023, sending USD 22.2 billion in cryptocurrencies to different services (Naqbi et al., 2025).

Even though anti-money laundering tactics have been the subject of much research, little is known about the function of regulatory technology (RegTech) and how it affects the efficiency of AML systems (AMLSE). Meanwhile, Rafiq and Sohail (2025) found that technological and organizational enablers had a beneficial impact on both RegTech adoption and AMLSE. Organizational constraints have an indirect impact on AMLSE, whereas technological barriers inhibit RegTech adoption. Mediation research emphasizes the importance of technological and organizational enablers in improving AMLSE through RegTech adoption. The moderated analysis sheds light on the intricate interconnections between motives for RegTech adoption and various enablers. The study demonstrates that banks' use of RegTech improves AML compliance by automating compliance processes, enhancing transaction monitoring, and allowing regulators to make quick modifications, resulting in increased AMLSE.

Figure 6 below demonstrates the must-have features of RegTech solutions.

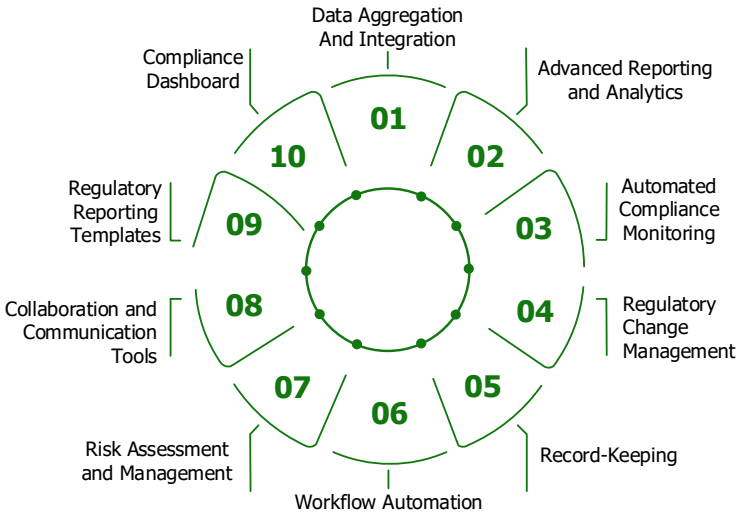

Figure 6. Must-have features of RegTech solutions. *(Source: Dill, 2021)*

Collaboration and innovation are seen as critical components in the creation and advancement of AML regulatory technologies (Vijayagopal et al., 2024; Eghaghe et al., 2024). Regulators and financial institutions are actively working together to investigate the use of artificial intelligence, machine learning, and data analytics tools to enhance AML compliance efforts and risk management processes (Moncalvo et al., 2025; Dote-Pardo & Espinosa-Jaramillo, 2025). This collaboration encourages the exchange of knowledge, best practises, and regulatory guidelines in order to remain ahead of evolving dangers and needs. To improve the effectiveness of financial monitoring design, explore a collaborative strategy involving politics, academia, and businesses.

Financial institutions conduct risk assessments to examine their exposure through their customers, routes of operation, and services they provide. Observations of over 100 market solutions show that very few of these solutions have regulatory intellectual property in two forms: risk assessment-based typologies and direct linkages to applicable regulatory requirements within the detection solution (Gupta & Kaur, 2024). The bulk of solutions available for an FI to handle all of the risks it is exposed to and all typologies it has to monitor are toolboxes, which need a large amount of trial and error and time to yield concrete results. Apart from removing false positives from legacy solutions, which is the first noticeable improvement, ongoing incremental improvements are modest.

Furthermore, studies demonstrate that RegTech solutions suffer from a lack of interpretability and explanation in their results/outcomes (interpretability is the degree to which a cause-and-effect relationship can be detected within a system, allowing one to predict what will happen given a change in input or algorithmic parameters). Explainability refers to the degree to which the underlying workings of a machine or algorithm can be explained in human words (Abikoye et al., 2024; Siering, 2022). The interpretability and explainability of results are equally crucial in ensuring transparency in a solution.

Most solutions are either adequately interpretable or explainable, but not both. This is a dilemma for FIs because the alerts and forecasts provided by such systems are either incomprehensible or explainable to the business users and investigators who deal with them. As a result, it does not enhance the current information accessible to alert investigators so that they can properly examine and dispose of an alert generated by the FI's detection solution. AI solutions built on blackbox models that lack transparency will not withstand regulatory scrutiny.

There is clearly an increasing demand for domain expertise and shared learning in RegTech. Despite technological and machine learning advancements, it will take some time before regulators can build a regulatory framework or even offer standards. As a result, RegTech solutions will continue to be constrained by a lack of regulatory guidance and domain expertise in AML/CFT and fraud, limiting their capacity to fully leverage the potential of AI and technology for efficient monitoring. To assist banks in mitigating all known financial crime threats, new solutions must be designed with regulatory standards in mind, supplemented by comprehensive typology libraries that are regulatory-compliant.

Actually, banks must transition to transaction monitoring 2.0 (McKinsey&Company, 2019), which offers the best alert optimization and detection quality. While enhancing rule-based systems with RegTech can assist in reducing some of the operational overhead associated with responding to alarms, banks must expand their present usage of machine learning

DOI: 10.55643/fcaptp.3.68.2026.5184

to improve detection. Because hiring a vendor solution to just optimize alerts is costly, FIs should examine more cost-effective alternatives, such as in-house solutions built with open-source technologies.

Actually, these processes of development and continuous adjustments can be called 'Agile RegTech', the pillars of which are agility, speed, integration, and analytics.

DISCUSSION

Financial monitoring in the banking system is widely recognized both by scholars and practitioners of the financial/banking sector as a crucial instrument for ensuring the economic security of the state. Nevertheless, scholars emphasize several fundamental contradictions that complicate its effective implementation. One central tension arises between the need for comprehensive oversight and the protection of client rights. Banks are mandated to identify suspicious transactions to prevent money laundering and terrorist financing, yet excessive monitoring may slow down transaction processing, generate false positives, and raise privacy concerns. Current research highlights the potential of RegTech to optimize monitoring processes, enhancing efficiency while minimizing intrusive interventions (Gasparri, 2019). This is also, in fact, in line with our findings.

Another key contradiction exists between the rapid pace of financial innovation and the capacity of regulatory frameworks to adapt. The growth of digital banking, online payment systems, and emerging financial instruments such as cryptocurrencies introduces new risks to the economic security of the state. Traditional monitoring mechanisms often lag behind these developments. RegTech solutions offer automated compliance, real-time transaction analysis, and adaptive reporting systems, yet their implementation requires substantial investment and organizational restructuring, raising debates over feasibility and scalability (Ho & Jung, 2024). According to Bagherifam et al. (2025), by improving accountability, expediting reporting, and fortifying governance networks throughout the public-private interface, RegTech and SupTech solutions generate substantial administrative value. However, organizational opposition, algorithmic opacity, regulatory fragmentation, and cybersecurity flaws limit implementation. The paper suggests an integrated governance framework that charts potential and obstacles in the areas of institutional coordination, risk, compliance, and technology in order to address these problems. By combining disparate pieces of data, this study advances the area of administrative sciences by presenting RegTech and SupTech as transformative tools of digital public administration and regulatory modernization, in addition to being technological developments.

A further challenge is the conflict between standardization and local regulatory requirements. International frameworks, such as FATF recommendations and Basel Committee guidelines, promote harmonization of monitoring practices; however, national authorities impose specific legal and operational requirements reflecting local economic and risk environments. Scholars argue that RegTech can facilitate simultaneous compliance with both international and domestic regulations, but discussions continue regarding its practical effectiveness in reconciling these sometimes-divergent demands (Salampasis & Samakovitis, 2024).

In addition, there is a persistent contradiction between reactive and proactive approaches to economic security. Conventional monitoring often functions reactively, detecting irregularities after transactions occur. Advanced RegTech tools, incorporating artificial intelligence and big data analytics, enable predictive and proactive approaches, allowing banks to anticipate and prevent potentially risky operations. Nonetheless, concerns remain about algorithmic reliability, transparency, and the assignment of accountability in automated decision-making processes.

Finally, a broader tension exists between ensuring state-level economic security and maintaining the freedom and efficiency of business activity. While stringent monitoring strengthens protection against financial crimes, it may inadvertently hinder entrepreneurial initiatives, particularly in small and medium-sized enterprises. RegTech mitigates this tension by automating compliance processes, reducing administrative burdens, and improving operational efficiency. Yet, scholars emphasize that technology alone cannot fully resolve the inherent contradictions in financial monitoring, and careful design of both regulatory and organizational frameworks remains essential.

In summary, RegTech plays a pivotal role in addressing these contradictions, offering enhanced automation, predictive analytics, regulatory adaptability, and cost reduction. At the same time, ongoing research underscores ethical, operational, and governance challenges, highlighting the need for a balanced integration of technological solutions into the broader financial monitoring framework.

Most scholarly studies today are concentrated in the domain of preventing financial fraud and data leakage in digital banking (Gaviyau & Godi, 2025; Iyelolu et al., 2024). However, more complex and latent factors – those of geopolitical and geoeconomic nature – usually appear out of sight.

In the meantime, to improve cyber resilience and protect financial stability in a changing geopolitical environment, international cooperation and forward-thinking policies are required. Investigating how improved cyber resilience might enhance current AML/CFT standards and strengthening alliances at all levels through means like reciprocal assessments or public-private collaboration should be top priorities. Additional research would concentrate on ex ante measures that lessen the probability and impact of cyber incidents, such as bolstering the governance of cyber risk and the resilience of vital data centers and cloud services, even though AML/CFT frameworks primarily address illicit financial flows after entry into the financial system. In addition to helping to avoid and mitigate cyber-related vulnerabilities, this endeavor would support the global agenda on financial crime and cyber resilience, including dangers in crypto-asset markets and state-linked "crypto hijacking" in the context of sanctions evasion.

Cloud computing, Application Programming Interfaces (APIs), and real-time data analytics are becoming more and more important to banks, securities firms, payment providers, and market infrastructures. Other significant trends are the spread of digital assets and the quick use of AI. BigTech businesses and non-bank financial intermediaries are increasingly involved in offering asset management, credit, and payment services. These advancements increased accessibility to financing and increased efficiency, but they also increased the risk of cyberattacks and produced new reliance on digital infrastructures. These hazards may be increased by geopolitical conflicts. Cyber operations that are specifically targeted can be used to send political messages, evade sanctions, or interfere with cross-border capital flows. In this situation, financial institutions, especially those engaged in cross-border payment and settlement, become desirable targets. Recent conflict-related episodes show how cyber activity can spike during times of increased geopolitical stress, affecting not only financial institutions but also vital infrastructures that facilitate capital flows and trade.

Cyber invasions play a major role in many significant thefts from the crypto-asset ecosystem, as seen by the frequent instances of "crypto hijacking", in which attackers obtain unauthorized control over crypto-asset exchanges, wallets, or other digital asset service providers. In these situations, stolen assets are usually transferred between jurisdictions and through a variety of obfuscation methods before reentering the financial system, making AML/CFT oversight and the application of sanctions more difficult. From a policy standpoint, this would suggest that AML/CFT measures frequently only become effective after stolen assets begin to circulate, highlighting the significance of proactive cybersecurity and prudent operational risk management at exchanges, wallet providers, and other vital service providers.

A new workstream would aim to improve ex ante cyber resilience to reduce the possibility that intrusions into IT systems, data centers, and digital asset platforms will result in significant losses of data or funds, even though AML/CFT frameworks and standards primarily address illicit financial flows after they enter the financial system. The strategy is in line with global initiatives on financial crime and cyber resilience. First, by looking at how strong operational and cyber defenses, such as good governance and insider-risk management, can lessen prospects for sanctions evasion, cyber-enabled money laundering, and the misuse of cryptocurrency assets. Second, by drawing attention to the sectoral and macro-financial avenues via which successful attacks can spread.

Geopolitical dynamics and cybersecurity concerns are becoming more entwined. These days, organized cybercrime syndicates and organization-driven intelligence organizations are frequently linked to attacks intended to accomplish more than just resource theft; they also serve more general strategic goals. These could involve influencing political talks, putting pressure on sanctions episodes, interfering with cross-border payment networks, or eroding confidence in a competitor's financial system. In this way, financial cybersecurity has evolved from a technical/operational or compliance issue to a field of international security strategy.

Cyber operations can be targeted to disrupt supply chains and create economic pressure instead of just extracting money, as demonstrated by attacks like the 2017 NotPetya ransomware, which paralyzed Ukrainian businesses and public institutions and had global repercussions. In general, cyberattacks tend to coincide with times of increased geopolitical tension, highlighting their function as instruments of strategic power.

Developing regional data centers to gather and exchange information on cyber incidents and policy responses, when appropriate, and performing mutual evaluations to reflect features of cyber resilience are examples of potential policy alternatives. Tracking progress and identifying new gaps can be facilitated by regular exercises and improved tools for tracking cyber resilience and associated financial crime threats. When combined, these initiatives can help guarantee that digitalization yields all of its advantages while maintaining the reliability and integrity of financial markets.

Overall, the conducted systematic literature review demonstrates that financial monitoring in the banking sector is undergoing a profound transformation driven by digitalization, geopolitical instability, cyber threats, and the increasing complexity of global financial ecosystems. Unlike traditional approaches that primarily interpreted financial monitoring as a com-

DOI: 10.55643/fcaptp.3.68.2026.5184

pliance-oriented mechanism aimed at preventing money laundering and terrorist financing, contemporary research increasingly conceptualizes monitoring systems as multidimensional instruments of economic resilience and state security (Kulikov, P. et al., 2022). One of the principal findings of the review concerns the growing convergence between financial monitoring, cybersecurity, and economic sovereignty. The literature consistently indicates that modern financial infrastructures are becoming deeply dependent on digital technologies, cloud services, cross-border data flows, artificial intelligence, and interconnected financial platforms. While these transformations increase operational efficiency and financial inclusion, they simultaneously generate systemic vulnerabilities capable of destabilizing national economies and undermining institutional trust. As a result, financial monitoring increasingly functions not only as a mechanism of regulatory compliance but also as a strategic component of national security architecture.

The review additionally reveals a significant shift from traditional rule-based transaction monitoring systems toward adaptive and predictive monitoring models based on artificial intelligence, machine learning, and advanced analytics. Scholars emphasize that these technologies substantially improve the speed, scalability, and accuracy of suspicious activity detection. However, the analysis simultaneously identifies major concerns regarding algorithmic opacity, explainability, accountability, and ethical governance of AI-driven systems. This contradiction illustrates a broader dilemma within the contemporary financial monitoring environment: technological innovation strengthens monitoring capabilities while simultaneously creating new governance and security risks.

Another important pattern identified in the literature concerns the increasing fragmentation of regulatory environments. Although international organizations such as the Financial Action Task Force (FATF), International Monetary Fund (IMF), and Financial Stability Board (FSB) promote harmonized standards for AML/CFT regulation and financial supervision, significant discrepancies persist across national jurisdictions. This fragmentation complicates cross-border monitoring, increases compliance costs, and creates opportunities for regulatory arbitrage. The findings therefore support the argument that effective financial monitoring increasingly depends on international coordination, institutional interoperability, and integrated governance mechanisms.

The analysis further demonstrates that geopolitical dynamics became one of the central determinants shaping the evolution of financial monitoring systems. Contemporary financial monitoring is increasingly influenced by sanctions regimes, hybrid threats, cyber warfare, strategic competition between states, and the weaponization of financial infrastructures. Cyberattacks targeting payment systems, digital assets, and financial institutions demonstrate that economic security and cybersecurity are becoming structurally interconnected domains. Consequently, financial monitoring should no longer be interpreted exclusively within the framework of financial compliance but rather as part of broader state resilience strategies under conditions of geopolitical uncertainty.

The review also identifies a persistent tension between strengthening financial security and maintaining operational flexibility of banking institutions. Stricter AML/CFT requirements improve transparency and reduce systemic risks but simultaneously increase administrative burdens, compliance expenditures, and operational rigidity. Small and medium-sized financial institutions may experience disproportionate pressure due to limited technological and organizational resources. In this context, RegTech solutions emerge as important instruments capable of partially reconciling regulatory effectiveness with operational efficiency through automation, predictive analytics, and real-time compliance mechanisms. An important theoretical implication of this study lies in demonstrating that financial monitoring should be conceptualized as a systemically integrated and multidimensional governance mechanism operating at the intersection of technological innovation, institutional regulation, cybersecurity, and geopolitical security. Existing literature often examines these dimensions separately, which contributes to analytical fragmentation. The proposed integrative perspective allows for a broader understanding of how financial monitoring contributes to the resilience and stability of contemporary economic systems.

The study also has important practical implications. The findings indicate that policymakers and regulatory authorities should prioritize the development of adaptive, technologically integrated, and internationally coordinated monitoring frameworks. Particular attention should be devoted to improving cyber resilience, strengthening cross-border regulatory cooperation, increasing transparency of AI-driven monitoring systems, and integrating cybersecurity governance into AML/CFT strategies. Financial institutions, in turn, should focus on developing scalable monitoring infrastructures capable of combining operational flexibility with regulatory compliance and systemic risk mitigation.

Despite the contributions of the study, several limitations should be acknowledged. The analysis is primarily based on qualitative synthesis of interdisciplinary literature and does not include quantitative meta-analysis due to the heterogeneity of existing studies. Furthermore, the rapidly evolving nature of digital finance and cybersecurity implies that regulatory practices and technological solutions may continue to change significantly after the completion of the review. Future research may therefore focus on empirical evaluation of AI-driven monitoring effectiveness, comparative analysis of national supervisory models, and scenario-based assessment of geopolitical cyber risks within financial systems.

Overall, the findings confirm that financial monitoring in the banking sector is evolving into a strategic and adaptive mechanism of economic security governance. Its future effectiveness will depend on the ability of states, regulators, and financial institutions to balance technological innovation, operational resilience, regulatory coordination, and protection of economic sovereignty within an increasingly unstable and digitized global environment.

The presented research is limited to conceptual qualitative analysis. But in the future, more policy studies might concentrate on helping decision-makers better grasp new threats at the nexus of geopolitical dynamics and cyber risk, as well as their potential effects on the financial industry and the actual economy. Granular evaluations of cross-border interdependencies in financial-sector ICT supply chains, scenario-based modeling of severe but plausible cyber shocks, and comparative analyses of supervisory practices and governance approaches for cyber resilience in finance in the era of AI are some examples of this. The goal is to give policymakers a more solid body of evidence to assess and adjust their policy approaches.

CONCLUSIONS

The conducted systematic literature review demonstrates that financial monitoring in the banking sector has evolved from a narrowly specialized compliance mechanism into a strategic and multidimensional component of state economic security architecture. Contemporary monitoring systems increasingly operate at the intersection of financial regulation, cybersecurity, technological innovation, geopolitical stability, and institutional governance. The findings confirm that the digital transformation of financial systems significantly reshapes the operational logic of financial monitoring. Artificial intelligence, machine learning, predictive analytics, and RegTech solutions are progressively replacing traditional rule-based monitoring approaches and enabling adaptive, real-time, and data-driven risk management. These technological transformations substantially improve the effectiveness of suspicious activity detection and strengthen the resilience of financial systems. At the same time, they generate new categories of systemic risk associated with cyber vulnerabilities, algorithmic opacity, data governance, and institutional dependence on digital infrastructures.

The study identified five dominant thematic clusters within the contemporary literature: technological transformation of monitoring systems; AML/CFT regulatory evolution; cyber resilience and operational security; institutional and governance mechanisms; and geopolitical determinants of financial stability. The synthesis of these research streams demonstrates that financial monitoring should be interpreted not as an isolated supervisory function but as an integrated mechanism embedded within broader national and international security architectures.

Moreover, the review revealed several systemic contradictions that shape the modern monitoring environment. These include tensions between technological innovation and regulatory adaptability, transparency and privacy protection, automation and explainability, globalization and economic sovereignty, as well as security objectives and operational flexibility of financial institutions. The coexistence of these contradictions confirms the growing complexity of financial monitoring systems under conditions of accelerated digitalization and geopolitical instability.

An important contribution of the study lies in the development of an integrated conceptual understanding of financial monitoring as a strategic instrument of economic resilience. The findings demonstrate that contemporary monitoring systems increasingly perform functions extending beyond AML/CFT compliance, including protection of financial stability, mitigation of cyber risks, support of institutional trust, and strengthening of national economic sovereignty. The practical implications of the research indicate the necessity of developing adaptive and internationally coordinated monitoring frameworks capable of integrating cybersecurity governance, AI-based analytics, and cross-border regulatory cooperation. Policymakers should prioritize the improvement of institutional interoperability, transparency of algorithmic systems, and resilience of critical financial infrastructures. Financial institutions, in turn, should focus on scalable and technologically integrated monitoring architectures that combine operational efficiency with effective risk management.

The study also highlights the growing strategic significance of geopolitical factors in shaping financial monitoring systems. Hybrid threats, sanctions regimes, cyber warfare, and transnational financial flows increasingly influence both regulatory practices and the architecture of financial security governance. Consequently, financial monitoring becomes an essential instrument for protecting economic sovereignty and maintaining national resilience under conditions of global instability.

Future research may further expand empirical investigation of AI-driven monitoring systems, comparative analysis of national supervisory approaches, and scenario-based modeling of cyber-financial risks. Additional attention should also be devoted to the interaction between digital assets, decentralized finance, and emerging regulatory mechanisms within the evolving global financial system.

DOI: 10.55643/fcaptp.3.68.2026.5184

Overall, the study confirms that the future effectiveness of financial monitoring will depend on the ability of states and financial institutions to balance technological innovation, cybersecurity resilience, regulatory coordination, and protection of economic sovereignty in an increasingly interconnected and volatile financial environment.

To summarize, changes are needed in the transaction monitoring area to detect money laundering operations with greater precision and efficiency. Researchers must continue to investigate improved solutions. Although there are hurdles to overcome and more research is required, AML specialists' insights and opinions indicate that technology such as machine learning will significantly improve the area. Adopting and appropriate adapting artificial intelligence and machine learning will not only increase money laundering detection, but will also pave the way for more inventive and enhanced ways that can solve the anti-money laundering industry's constantly changing difficulties.

ADDITIONAL INFORMATION

AUTHOR CONTRIBUTIONS

All authors have contributed equally.

FUNDING

The Authors received no funding for this research.

CONFLICT OF INTEREST

The Authors declare that there is no conflict of interest.

REFERENCES

1. Abikoye, B., Umeorah, S., Adelaja, A., Ayodele, O., & Ogunsuji, Y. (2024). Regulatory compliance and efficiency in financial technologies: Challenges and innovations. *World Journal of Advanced Research and Reviews, 23*(1), 1830-1844. https://doi.org/10.30574/wjarr.2024.23.1.2174
2. Adegbite, M. (2025). Data privacy and data security challenges in digital finance. *Journal of Digital Security and Forensics, 2*(1), 6-19. https://doi.org/10.29121/digisecforensics.v2.i1.2025.40
3. Akinbowale, O. E., Klingelhöfer, H. E., Zerihun, M. F., & Mashigo, P. (2023). Development of a policy and regulatory framework for mitigating cyberfraud in the South African banking industry. *Heliyon, 10*(1), e23491. https://doi.org/10.1016/j.heliyon.2023.e23491
4. Akiotu, H. (2022). Bank management compliance strategies to avoid regulatory sanctions (Doctoral dissertation, Walden University). Walden Dissertations and Doctoral Studies. https://scholarworks.waldenu.edu/dissertations/11489/
5. Ali, A. H. (2019). A survey on vertical and horizontal scaling platforms for big data analytics. *International Journal of Integrated Engineering, 11*(6), 138-150. https://publisher.uthm.edu.my/ojs/index.php/ijie/article/view/2892
6. AlQudah, A., Hailat, M., & Setabouha, D. (2025). Money Laundering in Global Economies: How Economic Openness and Governance Affect Money Laundering in the EU, G20, BRICS, and CIVETS. *Journal of Risk and Financial Management, 18*(6), 319. https://doi.org/10.3390/jrfm18060319
7. Anil, V., & Bobatope, A. (2024). Data privacy, security, and governance: A global comparative analysis of regulatory compliance and technological innovation. *Global Journal of Engineering and Technology Advances, 21*(03), 190-202. https://doi.org/10.30574/gjeta.2024.21.3.0246
8. Antwi, S., Tetteh, A., Armah, P., Dankwah, E. (2023). Anti-money laundering measures and financial sector development: Empirical evidence from Africa. *Cogent Economics & Finance, 11*(1), 2209957. https://doi.org/10.1080/23322039.2023.2209957
9. Athari, S., Irani, F., & Al Hadood, A. (2023). Country risk factors and banking sector stability: Do countries' income and risk-level matter? Evidence from global study. *Heliyon, 9*(10), e20398. https://doi.org/10.1016/j.heliyon.2023.e20398
10. Bagherifam, N., Naghdi, S., Ahmadian, V., Fazlzadeh, A., & Baghalzadeh Shishehgarkhaneh, M. (2025). Digital Regulatory Governance: The Role of RegTech and SupTech in Transforming Financial Oversight and Administrative Capacity. *International Journal of Financial Studies, 13*(4), 217. https://doi.org/10.3390/ijfs13040217
11. Bardin, P., Bouveret, A., Jackson, G., & Markevych, M. (2023, September 4). Money laundering poses a risk to financial sector stability: Curbing cross-border illicit proceeds demands a united global effort and innovative approaches. *IMF Blog*. https://www.imf.org/en/blogs/articles/2023/09/04/money-laundering-poses-a-risk-to-financial-sector-stability
12. Bisetti, E. (2024). The value of regulators as monitors: Evidence from banking. *Management Science, 70*(12). https://doi.org/10.1287/mnsc.2021.03083
13. Carretta, A., Cucinelli, D., Fattobene, L., & Schwizer, P. (2025). Bank misconduct: The deterrent effect of country

governance and customer reaction. *Journal of Banking & Finance, 174*, 107434. https://doi.org/10.1016/j.jbankfin.2025.107434

14. Chitimira, H., & Munedzi, S. (2023). Overview international best practices on customer due diligence and related anti-money laundering measures. *Journal of Money Laundering Control, 26*(7), 53–62. https://doi.org/10.1108/JMLC-07-2022-0102
15. Chronopoulos, D., Wilson, J., & Yilmaz, M. (2023). Regulatory oversight and bank risk. *Journal of Financial Stability, 64*, 101105. https://doi.org/10.1016/j.jfs.2023.101105
16. de Weijer, S., Leukfeldt, R., & Moneva, A. (2024). Cybercrime during the COVID-19 pandemic: Prevalence, nature and impact of cybercrime for citizens and SME owners in the Netherlands. *Computers & Security, 139,* 103693. https://doi.org/10.1016/j.cose.2023.103693
17. de Willebois, E. V. D. D., Sharman, J. C., Harrison, R., Park, J. W., & Halter, E. (2011). *The puppet masters: How the corrupt use legal structures to hide stolen assets and what to do about it*. World Bank Publications. https://documents1.worldbank.org/curated/en/784961468152973030/pdf/The-puppet-masters-how-the-corrupt-use-legal-structures-to-hide-stolen-assets-and-what-to-do-about-it.pdf
18. Demirguc-Kunt, A., & Detragiache, E. (2000). Monitoring Banking Sector Fragility. *The World Bank Economic Review, 14*(2), 287-307. https://www.researchgate.net/publication/233568340_Monitoring_Banking_Sector_Fragility
19. Devi, M. (2025). The Evolution of Financial Regulation: A Historical Overview. *International Journal of Creative Research Thoughts, 13*(3), 728-742. https://www.ijcrt.org/papers/IJCRT25A3128.pdf
20. Dissanayake, H., Popescu, C., & Iddagoda, A. (2023). A bibliometric analysis of financial technology: Unveiling the research landscape. *FinTech*, *2*(3), 527-542. https://doi.org/10.3390/fintech2030030
21. Dill, A. (2019). *Bank regulation, risk management, and compliance*. Informa Law.
22. Dill, A. (2021). *Anti-money laundering regulation and compliance: Key Problems and Practice Areas*. Edward Elgar Publishing.
23. Dote-Pardo, J., & Espinosa-Jaramillo, M. (2025). Money laundering risks of cryptocurrencies: Towards coordinated regulatory and technological strategies. *Latin American Journal of Central Banking*, 100194. https://doi.org/10.1016/j.latcb.2025.100194
24. D'Souza, J., & Madrekar, A. (2026, May 12). Money Laundering Statistics by Country, Types and Facts (2025). *ElectroIQ*. https://electroiq.com/stats/money-laundering-statistics/
25. Eghaghe, V., Osundare, O., & Okeke, Ch. (2024). Advancing AML tactical approaches with data analytics: Transformative strategies for improving regulatory compliance in banks. *Finance & Accounting Research Journal, 6*(10), 1893-1925. https://doi.org/10.51594/farj.v6i10.1644
26. EY (2025). Navigating the next wave of AML regulation to drive strategic innovation The role of AMLA. https://www.ey.com/content/dam/ey-unified-site/ey-com/en-nl/industries/banking-capital-markets/documents/fco/ey-fc-navigating-the-next-wave-of-aml-regulation.pdf
27. Gasparri, G. (2019). Risks and Opportunities of RegTech and SupTech Developments. *Frontiers in Artificial Intelligence, 2*, 14. https://doi.org/10.3389/frai.2019.00014
28. Gaviyau, W., & Godi, J. (2025). Emerging Risks in the Fintech-Driven Digital Banking Environment: A Bibliometric Review of China and India. *Risks*, *13*(10), 186. https://doi.org/10.3390/risks13100186
29. Gelle, V. (2024). Enhancing financial security: AI-driven anti-money laundering (AML) and compliance monitoring in the banking sector. *World Journal of Advanced Research and Reviews, 25*(01), 2462-2476. https://doi.org/10.30574/wjarr.2025.25.1.0365
30. Ghash, P., & Golder, U. (2026). Exploring the effects of FinTech adoption on traditional banking: A systematic literature review on opportunities and challenges. *Digital Business, 6*(1), 100163. https://doi.org/10.1016/j.digbus.2026.100163
31. Gupta, Ch., & Kaur, G. (2024). E-*banking, Fintech, & Financial Crimes: The Current Economic and Regulatory Landscape*. Springer.
32. Gupta, S. K., Nagar, N., & Srivastava, S. (2024). An Application of Structure Equation Modelling in Determinants of Customer Based Brand Equity (CBBE) in the Banking Area *Studies in Systems, Decision and Control*, *489,* 399-411. https://doi.org/10.1007/978-3-031-36895-0_32
33. Hanson, S., Ivashina, V., Nicolae, L., Stein, J. C., Sunderam, A., & Tarullo, D. (2024, March 28–29). The evolution of banking in the 21st century: Evidence and regulatory implications [Conference draft]. Brookings Papers on Economic Activity (BPEA) Conference. https://www.brookings.edu/wp-content/uploads/2024/02/6_Hanson-et-al_unembargoed_updated.pdf
34. Hilbers, P., Raaijmakers, K., Rijsbergen, D., & de Vries, F. (2013). Measuring the effects of financial sector supervision. DNB, Working Paper No. 388. https://www.dnb.nl/media/auoba4t1/working-paper-388.pdf
35. Ho, J., & Jung, H. (2024). RegTech and SupTech: the future of compliance. In J. Madir (Ed.). *FinTech* (pp. 369-396). Edward Elgar Publishing.
36. Hrytsenko, L., Zakharkin, O., Zakharkina L., Hedegaard, M., Kuznyetsova, A., & Novikova, L. (2024). Assessment Of The Level Of Information Transparency Of Banks. *Financial and Credit Activity Problems of Theory and Practice*, *6*(59), 60–75. https://doi.org/10.55643/fcaptp.6.59.2024.4619
37. Iyelolu, T., Agu, E., Idemudia, C., & Ijomah, T. (2024). Legal innovations in FinTech: Advancing financial services through regulatory reform. *Finance & Accounting Research Journal, 6*(8), 1310-1319. https://www.re-

DOI: 10.55643/fcaptp.3.68.2026.5184

searchgate.net/profile/Tochukwu-Ijomah-2/publication/383847839_Legal_innovations_in_FinTech_Advancing_financial_services_through_regulatory_reform/links/66dc4778b1606e24c21248d7/Legal-innovations-in-FinTech-Advancing-financial-services-through-regulatory-reform.pdf

38. Iyelolu, T. V., Agu, E. E., Idemudia, C., & Ijomah, T. I. (2024). Legal innovations in FinTech: Advancing financial services through regulatory reform. *Finance & Accounting Research Journal*, *6*(8), 1310-1319. https://doi.org/10.51594/farj.v6i8.1374

39. Karolyi, H., Mishchuk, H. Y., & Karpa, M. I. (2025). Military Migration and Demographic Transformations in Ukraine: Military Consequences for Territorial Communities. *Ukrainian Geographical Journal, 3*(131), 75–86. https://doi.org/10.15407/ugz2025.03.075

40. Koosakul, J., Zhang, L., & Zia, M. (2024). Geopolitical proximity and the use of global currencies. IMF Working Papers, *189*(2024). https://doi.org/10.5089/9798400287763.001

41. Korpela, S. J. (2025). Between a rock and a hard place: managing the conflict between anti-money laundering and financial inclusion. *Journal of Money Laundering Control, 28*(7), 65–80. https://doi.org/10.1108/JMLC-04-2025-0049

42. Kulikov, P., Anin, O., Vahonova, O., & Niema, O. (2022) Scientific and Applied Tools for Project Management in a Turbulent Economy with the Use of Digital Technologies. *IJCSNS. International Journal of Computer Science and Network Security*, *22*(9), 601-606. https://doi.org/10.22937/IJCSNS.2022.22.9.78

43. Kuznyetsova, A., Yefimenko, A., Pozovna, I., Koczar, J., Chub, A., Dobrovolska, O., & Panaseyko, I. (2025). The relationship between bank capitalization and socio-economic development: Evidence from European countries. *Banks and Bank Systems, 20*(2), 120-134. https://doi.org/10.21511/bbs.20(2).2025.10

44. Lessambo, F. (2023). *Fintech regulation and supervision challenges within the banking industry: A comparative study within the G-20*. Palgrave Macmillan.

45. LexisNexis Editorial Staff (2023). *Guide to Anti-Money Laundering & BSA Compliance*. LexisNexis.

46. Lysenko, S., Bobro, N., Korsunova, K., Vasylchyshyn, O., & Tatarchenko, Y. (2024). The role of artificial intelligence in cybersecurity: Automation of protection and detection of threats. *Economic Affairs*, *69*, 43-51. https://doi.org/10.46852/0424-2513.1.2024.6

47. McKinsey&Company (2019). *Transforming approaches to AML and financial crime*. https://www.mckinsey.com/~/media/mckinsey/business%20functions/risk/our%20insights/transforming%20approaches%20to%20aml%20and%20financial%20crime/transforming-approaches-to-aml-and-financial%20crime-vf.pdf

48. Moncalvo, D., & Oliva, M. (2025). Innovation practices and priorities in AML/CFT financial intelligence. *Journal of Money Laundering Control, 28*(4-5), 626–644. https://doi.org/10.1108/JMLC-05-2025-0063

49. Naqbi, Sh., Nobanee, H., & Ellili, N. (2025). Global trends and insights into cryptocurrency-related financial crime. *Research in International Business and Finance, 75*, 102756. https://doi.org/10.1016/j.ribaf.2025.102756

50. Nygaard, A., & Silkoset, R. (2023). Sustainable development and greenwashing: How blockchain technology information can empower green consumers. *Business Strategy and the Environment*, *32*(6), 3801-3813. https://doi.org/10.1002/bse.3338

51. Ohinok, S., & Kopylchak, M. (2024). International Cooperation in Combating Corruption and Money Laundering. *Economics of Systems Development, 6*(2), 156-162. https://doi.org/10.32782/2707-8019/2024-2-22

52. Olatinsu, O. (2024). AML Compliance Under Pressure: Balancing National Security and Financial Inclusion. *World Journal of Advanced Research and Reviews, 24*(1), 2783-2793. https://doi.org/10.30574/wjarr.2024.24.1.3133

53. Oztas, B., Cetinkaya, D., Adedoyin, F., Budka, M., Aksu, G., & Dogan, H. (2024). Transaction monitoring in anti-money laundering: A qualitative analysis and points of view from industry. *Future Generation Computer Systems, 159*, 161-171. https://doi.org/10.1016/j.future.2024.05.027

54. Patil, A., Mishra, B., Chockalingam, S., Misra, S., & Kvalvik, P. (2025). Securing financial systems through data sovereignty: a systematic review of approaches and regulations. *International Journal of Information Security, 24*(159). https://doi.org/10.1007/s10207-025-01074-4

55. Pavlidis, G. (2023). The dark side of anti-money laundering: Mitigating the unintended consequences of FATF standards. *Journal of Economic Criminology, 2*, 100040. https://doi.org/10.1016/j.jeconc.2023.100040

56. Pavlovskyi, O., Blikhar, M**.,** & Karpa, M. (2024). International migration in the context of financial and economic security: The role of public administration in the development of national economy, education, and human capital. *Edelweiss Applied Science and Technology*, *8*(6), 1492–1503. https://doi.org/10.55214/25768484.v8i6.2265

57. Pettersson Ruiz, E., & Angelis, J. (2021). Combating money laundering with machine learning–applicability of supervised-learning algorithms at cryptocurrency exchanges. *Journal of Money Laundering Control, 25*(4), 766–778. https://doi.org/10.1108/JMLC-09-2021-0106

58. Poliova, N., Polova, L., Stepanenko, S., Izmailov, Y., & Varenyk, V. (2024). Organizational and economic principles of financial monitoring of national business entities in the context of national security. *Edelweiss Applied Science and Technology, 8*(6), 1455-1466. https://doi.org/10.55214/25768484.v8i6.2262

59. Rafiq, M., & Sohail, M. (2025). Adopting regulatory technology for anti-money laundering in banking: Key enablers and barriers in a RegTech model. *Sustainable Futures, 10*, 101377. https://doi.org/10.1016/j.sftr.2025.101377

60. Ratnawati, K., Koval, V., Arsawan, I., Kazancoglu, Y., Lomachynska, I., & Skyba, H. (2024). Leveraging financial literacy into sustainable business performance: a mediated-moderated model. *Business, Management and Economics*

Engineering (BMEE), 22(2), 333-356. https://doi.org/10.3846/bmee.2024.21449

61. Rodríguez Valencia, L., Ochoa Arellano, M. J., Gutiérrez Figueroa, S. A., Mur Nuño, C., Monsalve Piqueras, B., Corrales Paredes, A. d. V., Bemposta Rosende, S., López López, J. M., Puertas Sanz, E., & Levi Alfaroviz, A. (2025). A Systematic Review of Artificial Intelligence Applied to Compliance: Fraud Detection in Cryptocurrency Transactions. *Journal of Risk and Financial Management, 18*(11), 612. https://doi.org/10.3390/jrfm18110612

62. Royde, N. (2022). Fintech and Anti-Money Laundering Regulation: Implementing a Regulatory Hierarchy Premised on Financial Innovation. *Texas A&M Law Review, 9*(2), 465. https://doi.org/10.37419/LR.V9.I2.5

63. Salampasis, D., & Samakovitis, G. (2024). Regtech Frontiers: Innovations, Trends, and Insights Redefining Compliance. In H. Baker, G. Filbeck, & K. Black (Ed.). *The Emerald Handbook of Fintech* (pp. 65-87). Emerald Publishing.

64. Shoetan, P., & Familoni, B. (2024). Transforming fintech fraud detection with advanced artificial intelligence algorithms. *Finance & Accounting Research Journal, 6*, 602–625. https://doi.org/10.51594/farj.v6i4.1036

65. Siering. M. (2022). Explainability and fairness of RegTech for regulatory enforcement: Automated monitoring of consumer complaints. *Decision Support Systems, 158*, 113782. https://doi.org/10.1016/j.dss.2022.113782

66. Slawotsky, J. (2020). Financial stability and national security in an era of hegemonic rivalry: The need to tighten United States securities disclosure requirements. *University of Pennsylvania Journal of Business Law, 22*(2), 457-491. https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1603&context=jbl

67. Srinivas, S., & Andal, C. (2023). Anti-money laundering (AML) issues in fintech. In *Emperor International Journal of Finance and Management Research* (Vol. IX, Issue IX, pp. 19–23). Mayas Publication. https://doi.org/10.5281/zenodo.17435779

68. Sultan, N., Mohamed, N., Chisunga, D., & Satar, A. (2025). The correlation of Financial Action Task Force recommendations: the perception of compliance officers concerning the deployment of third parties and Fintech for customer due diligence. *Journal of Money Laundering Control, 28*(2), 292–314. https://doi.org/10.1108/JMLC-08-2024-0135

69. Sydorchuk, O., Kharechko, D., Khomenko, H., & Kosarevych, N. (2024). Competencies for sustainable financial and economic management: Their impact on human capital development and national security. *Edelweiss Applied Science and Technology*, *8*(6), 1445-1454. https://doi.org/10.55214/25768484.v8i6.2261

70. Tanda, A., & Schena, C. M. (2019). *FinTech, BigTech and banks: Digitalisation and its impact on banking business models*. Springer.

71. Transaction Monitoring in Fintech Market Size, Share & Segmentation by Solution Type (2025, December). *S&S Insider*. https://www.snsinsider.com/reports/transaction-monitoring-in-fintech-market-9155

72. Turki, M., Hamdan, A., Cummings, R., Sarea, A., Karolak, M., & Anasweh, M. (2020). The regulatory technology "RegTech" and money laundering prevention in Islamic and conventional banking industry. *Heliyon, 6*(10), e04949. https://doi.org/10.1016/j.heliyon.2020.e04949

73. Verdier, P.-H. (2025). International Finance and the Return of Geopolitics. *American Journal of International Law, 119*(2), 1-111. https://doi.org/10.1017/ajil.2025.8

74. Viritha, B., Mariappan, V., & Venkatachalapathy, V. (2015). Combating money laundering by the banks in India: compliance and challenges. *Journal of Investment Compliance, 16*(4), 78-95. https://doi.org/10.1108/JOIC-07-2015-0044

75. Vijayagopal, P., Jain, B., & Ayinippully Viswanathan, S. (2024). Regulations and Fintech: A Comparative Study of the Developed and Developing Countries. *Journal of Risk and Financial Management, 17*(8), 324. https://doi.org/10.3390/jrfm17080324

76. Vuković, D. B., Dekpo-Adza, S., & Matović, S. (2025). AI integration in financial services: A systematic review of trends and regulatory challenges. *Humanities and Social Sciences Communications, 12*, 562. https://doi.org/10.1057/s41599-025-04850-8

77. Wang, Sh., Asif, M., Shahzad, M., & Ashfaq, M. (2024). Data Privacy and Cybersecurity Challenges in the Digital Transformation of the Banking Sector. *Computers & Security, 147,* 104051. https://doi.org/10.1016/j.cose.2024.104051

78. Windasari, N. A., Kusumawati, N., Larasati, N., & Amelia, R. P. (2022). Digital-only banking experience: Insights from gen Y and gen Z. *Journal of Innovation & Knowledge, 7*(2), 100170. https://doi.org/10.1016/j.jik.2022.100170

79. Zagorsky, V., Rahimov, F., Horbova, N., Zhuk, O., Pershko, L., & Mihus, I. (2023). Socio-economic Aspect of Territorial Organization of Power. *Economic Affairs (New Delhi), 68*(3), 1555-1564. https://doi.org/10.46852/0424-2513.3.2023.22

80. Zavoli, I., & King, C. (2021). The challenges of implementing anti-money laundering regulation: an empirical analysis. *The Modern Law Review*, *84*(4), 740-771. https://doi.org/10.1111/1468-2230.12628

DOI: 10.55643/fcaptp.3.68.2026.5184

Каролі Г., Будякова О., Акімова Л., Бортняк К., Шемаєва Л., Акімов О.

ФІНАНСОВИЙ МОНІТОРИНГ У БАНКІВСЬКІЙ СИСТЕМІ ЯК ІНСТРУМЕНТ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ДЕРЖАВИ

Стрімка цифрова трансформація глобального банківського сектора в поєднанні зі зростанням геополітичної нестабільності, кіберзагроз і складності транскордонних фінансових потоків суттєво посилила стратегічне значення систем фінансового моніторингу для забезпечення економічної безпеки держави. Сучасний фінансовий моніторинг виходить за межі традиційної комплаєнс-функції та дедалі більше функціонує як інтегрований механізм управління системними ризиками, фінансової стійкості та інституційної стабільності. Незважаючи на значну кількість досліджень, присвячених протидії відмиванню коштів (AML), фінансовим технологіям, кібербезпеці та регуляторним інноваціям, наукова література залишається фрагментованою та недостатньо інтегрованою до єдиної концептуальної рамки економічної безпеки. Метою дослідження є систематизація сучасних наукових підходів до фінансового моніторингу в банківській системі та визначення системних взаємозв'язків між механізмами фінансового моніторингу, технологічною трансформацією, кіберстійкістю та економічною безпекою держави. У дослідженні застосовано методологію систематичного огляду літератури на основі принципів PRISMA. Було проаналізовано наукові публікації, аналітичні звіти та інституційні дослідження, індексовані в провідних міжнародних базах даних, із використанням тематичного синтезу та порівняльного аналізу. Для поглибленого аналізу було відібрано 79 досліджень, що відповідали визначеним критеріям включення. Результати дослідження свідчать, що сучасні системи фінансового моніторингу еволюціонують у напрямі адаптивних, технологічно орієнтованих та інтенсивно керованих даними архітектур, які інтегрують штучний інтелект, машинне навчання, RegTech-рішення та предиктивну аналітику. Визначено п'ять домінантних тематичних кластерів: технологічна трансформація систем моніторингу; еволюція AML/CFT-регулювання; кіберстійкість та операційна безпека; інституційні та управлінські механізми; геополітичні детермінанти фінансової стабільності. Аналіз також виявив низку системних суперечностей, що формують сучасне середовище фінансового моніторингу, зокрема між інноваціями та регулюванням, прозорістю та приватністю, автоматизацією та пояснюваністю алгоритмів, глобалізацією та економічним суверенітетом. Наукова новизна дослідження полягає в розробці інтегрованої концептуальної рамки, яка розглядає фінансовий моніторинг як стратегічний компонент архітектури економічної безпеки держави в умовах цифрової трансформації та геополітичної нестабільності. Практичне значення роботи полягає у визначенні стратегічних напрямів підвищення ефективності фінансового моніторингу, посилення кіберстійкості та вдосконалення координації між державними органами, фінансовими установами та міжнародними регуляторними організаціями.

Ключові слова: фінансовий моніторинг, банківська система, AML/CFT, блокчейн, управління, інновації, економічна безпека, FinTech, RegTech

JEL Класифікація: G18, G21, F52, O33