

EVALUATING THE EFFICIENCY OF AUDITING FOR AML-CFT IN THE BANKING SECTOR

Zohr Babazada

Institute of Economics, Ministry of Science and Education, Baku, Azerbaijan
e-mail: babazadezohr@gmail.com

Abstract. This article researches the development phases and discusses the best practices for auditing in financial institutions. The article also identifies the use cases of new technologies such as artificial intelligence, data analytics and machine learning by the point of risk-based auditing.

Keywords: Audit, risk-based approach, financial monitoring, AML-CFT, banking.

BANK SEKTORUNDA ÇPY/TMM ÜZRƏ AUDİTİN EFFEKTİVLİYİNİN QIYMƏTLƏNDİRİLMƏSİ

Zöhr Babazadə

*İqtisadiyyat İnstitutu, Elm və Təhsil Nazirliyi, Bakı,
Azərbaycan*

Xülasə. Məqalədə maliyyə müəssisələri üzrə ÇPY/TMM sahəsində audit proseslərinin inkişaf istiqamətlərini araşdırılmış və ən yaxşı təcrübələr önə çıxarılmışdır. Bundan başqa məqalədə yeni texnologiyalar, həmçinin süni intellekt, data analitika və ya machine learning həllərinin tətbiqi istiqamətləri risk əsaslı audit baxımından araşdırılmışdır.

Açar sözlər: Audit, risk əsaslı yanaşma, maliyyə monitorinqi, ÇPY/TMM, bank sistemi.

ОЦЕНКА ЭФФЕКТИВНОСТИ АУДИТА ПО ПОД/ФТ В БАНКОВСКОМ СЕКТОРЕ

Зоһр Бабазаде

*Институт Экономики, Министерства Науки и
Образования, Баку, Азербайджан*

Резюме. В данной статье исследуются этапы развития и выделяются лучшие практики проведения аудита в финансовых учреждениях. Также рассматриваются примеры использования новых технологий, таких как искусственный интеллект, анализ данных и блокчейн-технологии, с точки зрения риск-ориентированного аудита.

Ключевые слова: Аудит, риск-ориентированный подход, финансовый мониторинг, ПОД/ФТ, банковская деятельность.

1. Introduction

Money Laundering and terrorism financing pose a significant threat to the security of the financial system worldwide. Such illicit flows should be identified in financial institutions and prevented in time. The concealment of such pending illegal flows gives strength to organized crime and terrorism, which hinders both economic development and security. Consequently, regulators have had to impose harsh anti-money laundering and counter-terrorist financing (AML-CFT) micromanagement on banks, making it as if such institutions are the first line in the war against the financing of terrorism and other related crimes [8]. Within banks, There are many layers of a bank's internal accounting integrated with auditing of compliance of AML/CFT activities, supervising internal control systems, processes and procedures that are intended to provide adequate compliance and effectiveness with such threats and completed audit processes and the bank regulatory relevant as well. These support mechanisms serve to determine sufficient controls and customer due diligence, as well as monitor and report

transactions to ensure that criminals do not abuse the banking system. There is, however, little doubt that the auditing issue concerning the AML aspects in a bank should receive more attention. The bank also faces the risk of significant monetary losses and loss of its image should it severely fail to implement an effective system of AML/CFT. In the past few years, many banks around the world have suffered monetary loss due to the enforcement for not following compliance. For example, a penalty of more than \$3 billion, which was imposed on TD Bank for failing to comply with the requirements of implementing necessary procedures on their AML program, resulted in them agreeing near the court of law in 2024. In that case, almost no internal control ensured that systems, time frames and audit recommendations captured resulted and did not serve as guidance to failure [15]. Conversely, practical audit functions can proactively identify and resolve compliance gaps before they enable financial crime. As regulators around the world (including the Financial Action Task Force, Basel Committee and national authorities) increase their scrutiny, banks have a compelling incentive to improve the efficiency of AML/CFT audits to mitigate the risk of sanctions and protect their reputations [11].

The existing AML/CFT compliance and auditing research highlights several key themes and discussions. One primary focus is the cost-effectiveness of AML initiatives. Banks allocate vast amounts of resources - global compliance expenditures reached approximately \$214 billion in 2020 [4] - yet the efficacy of the AML/CFT framework is frequently questioned. Research shows that despite substantial investments, authorities manage to intercept and recover less than 1% of illicit financial flows [7]. This discrepancy has led to discussions about enhancing the efficiency of AML/CFT controls to identify threats better, reducing false positives and unnecessary work while adhering to rigorous regulations. Another essential aspect is balancing rules-based and risk-based methodologies. Traditionally, banks operated with exhaustive, rules-based checklists (such as strict transaction monitoring protocols), ensuring compliance but often resulting in excessively high false-positive alert rates, frequently exceeding 90% [10]. In contrast, a risk-based approach - focusing resources on higher-risk customers, transactions and areas - is now championed as a global best practice to enhance efficiency. Adopting risk-based AML programs allows banks to allocate compliance efforts where the money laundering/terrorist financing risks are most remarkable, rather than uniformly treating all clients and transactions the same, thereby improving the impact per dollar spent [5].

Another key point in the literature is the role of technology and data analytics in improving AML/CFT auditing. There is broad consensus that traditional manual and rules-driven processes are inadequate against sophisticated laundering techniques [9]. These technologies can sift through massive transaction datasets more efficiently, detect unusual patterns that human auditors might miss and drastically reduce false alarms by learning to better distinguish truly suspicious behavior [9; 10]. However, implementing such tools requires

overcoming challenges in data quality, model interpretability and integrating AI insights into audit workflows - all of which are active discussion areas.

Debates arise on empowering internal auditors to flag issues without conflict of interest, especially in global banks where complex reporting lines can dilute accountability [12]. Some scholars have proposed new models (e.g., creating regional audit committees in global banks) to strengthen internal audit autonomy and oversight in AML/CFT matters [12].

2. Literature analysis and hypotheses extraction

Advanced analytics and AI can significantly improve AML/CFT audit efficiency - A widely echoed idea is that deploying data analytics, machine learning (ML) and artificial intelligence in AML monitoring and auditing will increase efficiency by reducing false positives and focusing investigative resources more effectively [11]. The context for this hypothesis is the current high false-positive rate in transaction monitoring - often, around 90-95% of alerts are not genuinely suspicious [10]. This creates a substantial operational burden on compliance staff who assess and investigate mostly apparent alerts. The hypothesis, supported by industry observations, is that analytics-driven auditing can pinpoint higher-risk customers and transactions with greater precision [11]. For example, banks in Singapore have reported good outcomes from integrating data analytics into their AML audit processes, allowing auditors to more sharply identify risky customer segments for closer review [11]. This hypothesis aligns with the broader digital transformation trend in compliance: it shows that technology acts as a force multiplier for auditors, increasing both the speed (efficiency) and quality (effectiveness) of AML/CFT audits. A pattern in the literature is a strong consensus - numerous sources prove innovation in AML through technology [9].

A strong internal audit function and governance framework enhances AML/CFT compliance efficiency - Many authors argue that the organizational setup and independence of the audit and compliance functions directly impact the effectiveness of AML/CFT controls [12]. The hypothesis is that when internal auditors are empowered, well-resourced and knowledgeable, they can identify control weaknesses early and ensure prompt remediation, thus improving the overall program efficiency (fewer gaps for regulators to find later and fewer costly incidents). Contextually, this ties to the “Three Lines of Defense” model: internal audit is the third line that independently evaluates the first (business units) and second line (compliance management) [6]. Basel Committee guidance explicitly notes that internal audit “plays an important role in independently evaluating [AML/CFT] risk management and controls” and recommends periodic, bank-wide AML/CFT audits with proactive follow-up on findings [6]. Several case studies support this; for instance, an internal audit in 2018 at TD Bank uncovered that the bank was using outdated high-risk jurisdiction lists and lacked processes to update monitoring rules [15].

Auditors' industry-specific skills are crucial drivers for successful implementation. Auditors should have specialized experience, required training hours, a balance in staffing,

investments in IT and productivity tools, compliant to firm regulations and a favorable ratio of audit hours to risk areas and phases. Experienced auditors excel at spotting and resolving potential challenges. Future research might investigate the elements influencing auditor capabilities and the supply of audit professionals [1].

Effective audit planning facilitates resource allocation and thorough risk assessment. To prioritize audit areas, evaluating each one against specific criteria and ranking them according to risk level is essential. This approach ensures strategic planning of audits by allocating resources to higher-risk areas. The study results show that audit planning in Ukrainian banks should apply a comprehensive risk assessment that considers internal and external factors. Thus, banks can quickly adapt to changes in their internal and external environments and allocate resources efficiently. It is necessary to develop a robust audit plan that includes a full risk assessment covering all key business processes and organizational units of the bank, where continuous risk monitoring will allow prompt adjustments to the audit plan in light of emerging threats or opportunities. The theoretical and practical foundations of audit planning through a risk-based approach serve as the framework for creating a banking risk assessment model [17].

Risk-oriented internal audits help address problems efficiently and this type of audit focuses on evaluating either insufficiently controlled or overly controlled risks. Additionally, risks are considered based on their significance, as represented on the Luckyert scale, which is minor, moderate and significant. But the materiality level may differ for each category; thus, it is essential to calculate the overall integral risk for the enterprise. The risk map of the financial department is constructed based on the concept of stakeholders. Research has demonstrated that the risk map facilitates monitoring risks associated with substantial distortions in accounting (financial) and non-financial reporting concerning responsibility centers [18].



Figure 1. Multi-Stage Framework for Internal Audit Planning

Source: [16]

Multi-stage framework for developing a robust internal audit plan - This new framework combines risk assessment of auditable units with the selection of audit activities and resource allocation using an integrated analytical hierarchy process (AHP), fuzzy comprehensive evaluation (FCE) and weighted multiple-choice goal programming (WMCGP) approach [16]. The model takes into account qualitative and quantitative decision criteria.

According to the framework, the initial stage involves the identification of potential risk items and corresponding audit activities. The subsequent risk assessment process assigns weights, levels and reduction values to each risk category. Finally, the estimation of resources and the prioritization of audit activities culminate in the development of an efficient internal audit planning roadmap.

The timing of audit investigations is also influenced by the principles of a risk-based approach. Nakamura et al. [13] demonstrated that the need for an audit increases significantly when conflicts of interest are present or when the intervention under review poses substantial risks, such as high levels of invasiveness or participant safety concerns. By contrast, factors such as study design and quality management practices exert a comparatively smaller influence on audit necessity. Importantly, the decision to initiate an audit should be context-specific and based on an evaluation of actual risk conditions [13].

Methodologically, this research adopts a structured comparative analysis that integrates academic literature, regulatory guidelines and case studies from the banking sector. To extend beyond descriptive review, the study also develops a new conceptual framework for evaluating the efficiency of AML/CFT auditing. The methodological steps are outlined as follows:

3. Methodology

The methodology of this research is based on a structured comparative analysis of academic literature, regulatory guidelines and case studies of the banking sector, complemented by the development of a new conceptual model for evaluating AML/CFT auditing efficiency. The methodological steps are as follows:

1. Case Study Analysis - Several international and regional banking cases were examined, including:

- TD Bank (2024) - fined over \$3 billion for AML compliance failures.
- Danske Bank (2018) - €200 billion laundering scandal, revealing audit inefficiencies.
- Azerbaijani bank - examined based on the professional experience of the author in the particular AML-CFT sector

Evaluation Criteria - To assess audit efficiency, three criteria were defined:

- Effectiveness - ability to detect genuine suspicious transactions (measured by reduction in false positives, number of Suspicious Transaction Reports (STRs) accepted by regulators).
- Efficiency - cost and resource allocation in auditing (audit hours per risk area, use of AI/ML tools, compliance budget allocation).

- Resilience - ability of audit systems to adapt to regulatory changes and new risks.

Comparative Approach - Using these criteria, practices across different jurisdictions were compared, highlighting gaps in current auditing methods and opportunities for innovation.

Model Development - Based on the findings, a Risk-Based Audit Efficiency Framework (RBAEF) was developed. This model integrates technology, governance and auditor skills into a structured system for improving AML/CFT audit outcomes.

To empirically examine how risk-based approaches can improve audit efficiency, a synthetic dataset of **100 financial transactions** was employed. Each transaction contained the following attributes:

- **transaction_id**: unique identifier for the transaction,
- **amount**: monetary value of the transaction,
- **transaction_type**: categorical label denoting whether the transaction was a purchase, transfer or withdrawal,
- **customer_id**: identifier of the customer initiating the transaction,
- **transaction_time**: timestamp of the transaction and
- **is_fraud**: binary target variable indicating whether the transaction was fraudulent (1) or legitimate (0).

Table 1. A sample excerpt of the dataset from Kaggle

transaction_id	amount	transaction_type	customer_id	transaction_time	is_fraud
1	1000	Purchase	1001	1/1/2023 10:00	0
2	1500	Transfer	1002	1/1/2023 11:00	1
3	2000	Purchase	1003	1/1/2023 12:00	0
4	3000	Withdrawal	1004	1/1/2023 13:00	0

Source: [14]

Preprocessing. The dataset was preprocessed to prepare it for model training:

- **Handling Missing Values** - any missing records were imputed using forward-fill methods.

- **Encoding Categorical Variables** - transaction types were converted into numeric form via label encoding, e.g., Purchase = 0, Transfer = 1, Withdrawal = 2.

- **Feature Engineering** - temporal features were extracted from the transaction timestamp, including hour of day, day of month, month and day of week. This was based on the hypothesis that fraud is not evenly distributed across time.

- **Normalization** - continuous features such as amount and customer_id was standardized using z-scores to ensure comparability with categorical features.

Model Training. A Random Forest Classifier was employed, owing to its robustness in handling mixed feature types and its proven effectiveness in fraud detection contexts. The dataset was split into training and testing sets (70%-30% split). The model was trained on the training set and evaluated on the test set.

To evaluate the efficiency of how machine learning tools can be very efficient to detect the fraud cases, we constructed a test model using 100 transaction entries. The model was trained and validated to distinguish between potentially fraudulent and non-fraudulent transactions. With a random state of 35, the performance results were as follows:

Table 2. Model Performance Metrics

Accuracy	0.93
Precision	0.83
Recall	1.00
F1-Score	0.91
ROC AUC Score	0.96

Model was correct 93% of the time in identifying transactions as either fraudulent or legitimate. An F1-Score of 0.91 shows an excellent balance between our model's ability to catch fraud without incorrectly flagging too many legitimate transactions. It's a more holistic measure of a model's performance than accuracy, especially when dealing with imbalanced datasets like fraud detection. ROC AUC score means there is a 96% probability that the model will assign a higher risk score to a randomly chosen fraudulent transaction than to a randomly chosen legitimate one. This shows our model has a very strong discriminatory power.

Table 3. Confusion Matrix

	Predicted Non-Fraud	Predicted Fraud
Actual Non-Fraud	18	2
Actual Fraud	0	10

The confusion matrix indicated that while two non-fraudulent transactions were misclassified as fraud (false positives), all fraudulent cases were correctly identified (true positives), demonstrating the model's effectiveness in minimizing the risk of overlooking fraud.

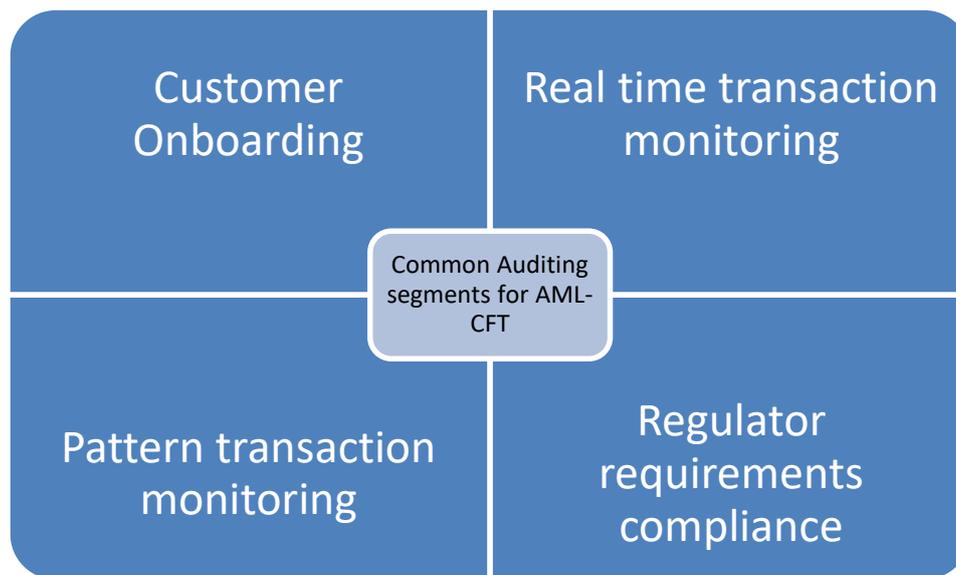
Furthermore, we tested the model on new transaction data. The results showed high fraud probabilities for certain high-value transactions (e.g., 87% and 84% likelihood of fraud), while routine transactions with lower amounts were classified as non-fraudulent with low probabilities.

These findings support the hypothesis that integrating RBA-based models can significantly enhance the efficiency of audit processes. In practice, this means that banking institutions can allocate audit resources more effectively - focusing on high-risk transactions rather than dispersing efforts across all activities. Such a selective approach not only reduces operational costs but also increases detection rates, contributing to stronger financial crime prevention systems.

4. Findings and discussion

Studies consistently demonstrate that integrating advanced data analytics and machine learning models enables auditors to identify suspicious patterns with higher precision, thereby reducing false positives and enhancing the allocation of investigative resources [9; 11]. By contrast, reliance on manual or rules-based processes often results in excessively high false-positive rates, which increase compliance costs without significantly improving detection outcomes [10].

Equally important is the role of internal auditors. Research highlights that empowered, well-resourced and knowledgeable audit teams are able to identify risk areas proactively, thereby mitigating the likelihood of regulatory penalties [12]. When auditors are adequately trained, supported with modern technological tools and organizationally independent, they contribute directly to the resilience of AML/CFT frameworks. This finding underscores the need for banks to prioritize auditor training, strengthen internal governance mechanisms and ensure that audit functions are not subordinated to conflicting managerial interests.



Graph 1. Common audited AML/CFT sectors

Source: Author's professional experience, Azerbaijani banking sector

Sector-specific expertise is also a critical determinant of audit effectiveness. As illustrated in Graph 1, AML/CFT auditing encompasses multiple domains, including customer onboarding, real-time transaction monitoring, pattern-based transaction monitoring and regulatory compliance. Each of these domains requires distinct knowledge bases and methodological approaches. For example, in the case of customer onboarding, auditors must assess whether client information is collected comprehensively, updated periodically and re-

screened against relevant sanctions lists whenever changes occur. Inadequate oversight of this process may result in sanctioned individuals or entities entering the financial system undetected.

In the area of real-time transaction monitoring, audit efficiency depends on calibrating the optimal number of transactions that a compliance officer can effectively review. A misalignment between alert thresholds and staff capacity often results in excessive false positives, which reduce both efficiency and morale. Conversely, underestimating the required monitoring volume may leave high-risk transactions undetected. Thus, auditors play a vital role in evaluating the balance between detection thresholds and operational feasibility.

Pattern-based transaction monitoring differs substantially from real-time monitoring because it relies on historical transaction data to identify long-term behavioral anomalies. For instance, regulators may require the reporting of customers conducting cryptocurrency transactions exceeding USD 10,000 on a monthly basis. In such cases, auditors must compare the organization’s software-generated alerts with regulatory expectations to ensure that suspicious transaction reports (STRs) are filed consistently and in compliance with applicable laws. Discrepancies between pattern analysis and actual reporting practices represent a critical area where auditors can intervene to strengthen compliance.

Regulatory requirements compliance is mandatory for organizations in their AML-CFT program. The auditors identify the sectors where risks might emerge or noncompliant patterns observed. This is especially the case for the scenarios where new AML law takes action in the field by the regulator. Predicting the possible risks after implementing the requirements is among the top skills auditors should have.



Graph 2. Process in internal auditing for AML-CFT

Source: [3]

Graph 2 illustrates the sequential process of internal auditing in the AML/CFT domain, beginning with the definition of objectives, followed by risk assessment, data preparation, execution of the audit and post-audit follow-up. Empirical studies confirm that the efficiency of this cycle depends heavily on the quality of the planning phase [3]. Limited resources necessitate the prioritization of high-risk areas, which requires auditors to perform comprehensive risk assessments covering both internal processes and external environmental factors.

During the execution stage, auditors are expected to maintain flexibility. Although audit plans are typically predetermined, emerging gaps may fall outside the original scope. In such cases, auditors should adjust their focus to address these gaps, in line with the principles of a risk-based approach. The post-audit stage is equally critical, as it involves synthesizing findings, issuing recommendations and ensuring that corrective actions are implemented effectively. Best practice requires that subsequent audit cycles include follow-up on past recommendations, thereby establishing a feedback loop that continuously strengthens the institution's AML/CFT framework.

Finally, the literature cautions against purely ad hoc auditing practices. While some scholars have proposed conducting audits only "when needed", evidence suggests that such an approach risk introducing bias and inconsistency in AML/CFT oversight [13]. Instead, regular, structured and risk-oriented auditing cycles provide greater assurance of compliance and long-term resilience.

Taken together, these findings confirm that the efficiency of AML/CFT auditing is determined by the integration of advanced technology, the empowerment and specialization of audit teams, rigorous audit planning and structured post-audit processes. By adopting such an approach, banks can significantly improve their ability to detect and prevent financial crime, thereby reducing regulatory risks and strengthening the integrity of the global financial system.

Conclusion. This study examined the efficiency of auditing practices in the AML/CFT domain, emphasizing the importance of a risk-based approach, sector-specific expertise and the integration of modern technologies such as artificial intelligence, machine learning and data analytics. While the literature demonstrates that traditional compliance strategies are often resource-intensive and prone to high false-positive rates, the findings of this research highlight pathways for enhancing both the efficiency and effectiveness of AML/CFT audits.

The methodological contribution of this study lies in its structured comparative analysis of international cases, regulatory guidelines and sector practices. Based on this foundation, the article proposes a new Risk-Based Audit Efficiency Framework (RBAEF), which integrates three core dimensions: (1) input factors such as regulatory requirements, data sources and institutional resources; (2) risk-based processes that combine technology, governance and auditor expertise and (3) measurable outputs in terms of detection accuracy, compliance costs

and resilience to regulatory change. By embedding a feedback loop into this framework, institutions can continuously refine their audit practices in response to emerging risks.

The originality of this contribution rests in its ability to operationalize the abstract concept of “efficiency” in AML/CFT auditing into a structured, measurable and adaptable framework. Unlike existing literature, which primarily discusses the role of technology or auditor independence in isolation, the proposed model consolidates these elements into a holistic system that can guide both practitioners and policymakers.

For the Azerbaijani banking sector in particular, applying this framework offers two key benefits: (i) improving audit efficiency by aligning limited resources with the highest-risk areas and (ii) strengthening compliance resilience in anticipation of evolving FATF and Basel Committee requirements. On a global level, the model provides regulators and financial institutions with a structured tool for benchmarking audit efficiency across different jurisdictions.

In conclusion, AML/CFT auditing is not merely a compliance exercise but a cornerstone of financial integrity and security. By adopting risk-based methodologies, leveraging advanced technologies (such as machine learning and AI) and applying structured frameworks such as the RBAEF, banks can enhance their ability to prevent financial crime, reduce regulatory exposure and safeguard trust in the financial system. Future research should test the proposed framework empirically within specific banking environments, using measurable indicators to further validate and refine its applicability.

References

1. Cardenas R.S., Ramel D.R. (2024), Application of risk-based audit approach by sole practitioners and local audit firms: Towards fully-compliant financial reports. *International Journal of Social Science and Education Research Studies*, Vol.4, No.11, 1257-1263. <https://doi.org/10.55677/ijssers/V04I11Y2024-10>
2. Hoffman B.N., Okeniyi J., Samuel S.E. (2024), Antecedents of compliance with anti-money laundering regulations in the banking sector of Ghana. *Journal of Risk and Financial Management*, Vol.17, No.8, 373. <https://doi.org/10.3390/jrfm17080373>
3. <https://amlyze.com/aml-audit/>
4. <https://seon.io/resources/aml-in-banking/>
5. <https://www.austrac.gov.au/business/core-guidance/preventing-financial-crime-using-risk-based-approach#:~:text=Why%20adopt%20a%20risk>
6. <https://www.bis.org/bcbs/publ/d353.pdf>
7. <https://www.fatf-gafi.org/en/topics/asset-recovery.html#:~:text=At%20the%20moment%2C%20countries%20intercept,border%20cases>
8. <https://www.imf.org/en/Topics/Financial-Integrity/amlcft>

9. <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-fight-against-money-laundering-machine-learning-is-a-game-changer>
10. <https://www.sipa.columbia.edu/detecting-financial-crimes-evaluating-efficacy-automated-transaction-monitoring#:~:text=However%2C%20most%20TMS%20used%20in,positive>
11. <https://www.theasianbanker.com/press-releases/abs-and-industry-group-launch-anti-money-laundering-audit-paper#:~:text=Harry%20Lim%2C%20group%20head%20of,mitigate%20the%20risks%20of%20money>
12. Naheem M. (2016), Internal audit function and AML compliance: The globalisation of the internal audit function. Journal of Money Laundering Control, Vol.19, No.4, 459-469. <https://doi.org/10.1108/JMLC-05-2015-0020>
13. Nakamura K., Saito A.M., Ueda K., Ueda K., Yoshihara K., Hiramatsu, N., Yamashita Y., Kusaka Y., Ui H. (2022), Risk-based approach to determine the need for an audit: In what situations should an audit be performed?. Rinsho yakuri/Japanese Journal of Clinical Pharmacology and Therapeutics, Vol.53, No.3, 49-53. https://doi.org/10.3999/jscept.53.3_49
14. Sadati H.M. (2024), AI fraud detection in auditing. <https://www.kaggle.com/datasets/heidarmirhajisadati/ai-fraud-detection-in-auditing>
15. Soltan L., Mclamb C. (2024), How to earn a \$3B fine: TD bank's masterclass in compliance failures. <https://www.corporatecomplianceinsights.com/how-earn-fine-td-bank-masterclass-compliance-failures/>
16. Wang X., Ferreira F.A.F., Pengyu Y. (2023), A multi-objective optimization approach for integrated risk-based internal audit planning. Annals of Operations Research, Vol.346, 1811-1840. <https://doi.org/10.1007/s10479-023-05228-2>
17. Дмишко Я. (2024), Ризик-орієнтований підхід до планування внутрішнього аудиту в банку. Облік і Фінанси, No.2, 100-105. [https://doi.org/10.33146/2307-9878-2024-2\(104\)-100-105](https://doi.org/10.33146/2307-9878-2024-2(104)-100-105)
18. Максимчук І., Уманець Т. (2021), Організація внутрішнього аудиту на підприємствах: Ризик-орієнтований підхід. Економіка. Фінанси. Право, No.8, 15-18. <https://doi.org/10.37634/efp.2021.8.3>