

Article

Counterparty Anti-Money Laundering Risk: A Three-Factor Matrix Model for Assessment and Control

Kiril Luchkov ^{1,*} and Nadya Velinova-Sokolova ²¹ Faculty of Management, Technical University of Sofia, 1000 Sofia, Bulgaria² Faculty of Economics and Business Administration, Sofia University “St. Kliment Ohridski”, 1113 Sofia, Bulgaria; nadya.sokolova@feb.uni-sofia.bg

* Correspondence: kiril.luchkov@tu-sofia.bg

Abstract

This study develops and applies a three-factor matrix model for assessing counterparty risk within Anti-Money Laundering (AML) measures. The research problem arises from the need to transform qualitative features related to ownership, effective control, economic logic of operations, geographical links, documents and review behavior into a comparable and documented risk score. The model uses three factors: counterparty exposure, transaction impact and control vulnerability. Each factor is assessed on a five-point ordered scale, and the overall risk score is obtained by multiplying the three values. The methodology includes scoring rules, rating interpretation, an application algorithm and a link between the profile, due diligence, ongoing monitoring and updating. The model was applied in 2026 to 25 anonymized counterparty profiles selected for methodological demonstration across different risk configurations. Identifying data, personal information and confidential business information were removed, while the relevant risk characteristics were preserved. The results demonstrate how the model distinguishes between low, moderate, increased, high and critical risk and how it creates a traceable link between established facts, numerical assessment and follow-up control actions. The study does not claim predictive accuracy, detection of money laundering or empirical validation against external AML outcomes. Its contribution is methodological and applied: it provides a transparent and explainable framework for structured, documented and proportionate management of counterparty AML risk, including potential use in AI-assisted monitoring under human oversight.

Keywords: anti-money laundering measures; counterparty risk; three-factor matrix model; risk-based approach; due diligence; AML compliance; artificial intelligence-assisted monitoring; automation; explainable risk assessment

Academic Editor: Marina Resta

Received: 11 June 2026

Revised: 28 June 2026

Accepted: 10 July 2026

Published: 20 July 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

1. Introduction

Risk assessment in AML measures is a core regulatory and internal-control requirement. It is not limited to customer identification, document collection or routine completion of internal forms. Its function is to determine whether a specific business relationship contains features that increase the need for due diligence, monitoring, escalation or refusal. From an AML perspective, the assessment does not prove wrongdoing. It identifies and documents the level of risk arising from the relationship between the counterparty, its ownership and control, its transactions, its behavior and the control environment.

The article is positioned primarily from the perspective of obliged entities that perform counterparty or customer due diligence, including financial institutions and other entities subject to AML controls. A risk-based approach requires differentiated and proportionate assessment. Counterparties cannot be treated equally when they differ in legal status, ownership structure, beneficial owner, sector of activity, geographical links, transaction value and frequency, payment method, source of funds, representation and degree of documentary transparency. Weak identification, inadequate beneficial ownership verification or insufficient ongoing monitoring may also expose an institution to regulatory, operational and reputational consequences, including enhanced supervisory scrutiny and broader jurisdictional consequences where AML weaknesses are systemic.

The main methodological problem is the transformation of qualitative information into a verifiable assessment. Assessing counterparty risk inevitably involves professional judgment. However, it must be consistent, comparable and documented. In the absence of a structured methodology, similar facts can lead to different assessments. This creates a risk of inconsistency, routine application of procedures and weak defensibility of the decision taken. The problem is not the mere presence of expert judgment. It is also related to the absence of a clear procedure that shows how professional judgment is formed, combined, classified and updated.

In the context of anti-money laundering measures, the described difficulty has direct managerial implications. The obliged entity must decide whether to establish a business relationship, how much information to collect, what checks to perform, what intensity of monitoring to apply and under what circumstances to update the assessment. Management decisions cannot be sustainable if they are based only on intuitive judgment. Therefore, a model is needed that links the established facts to a final risk profile and subsequent control actions.

This article proposes the three-factor matrix model as a semi-quantitative framework for assessing commercial counterparties. The semi-quantitative nature of the model means that qualitative features are converted into assessment values. These values do not measure risk with mathematical precision but create an ordered basis for comparison, classification and management decision. The model does not replace professional judgment but structures the order in which it is performed. By means of predefined factors, assessment values and predefined classification thresholds, the risk profile of the counterparty is derived.

In practice, risk may arise from the entity, but the way in which it participates in specific transactions is also important. In these cases, the economic logic of the transactions, the transparency of ownership, the source of funds, payment behavior, connections with certain jurisdictions, the refusal to cooperate and the discrepancy between the declared and actual circumstances are of great importance. Therefore, the subject of assessment is not only the counterparty itself but also the combination of the counterparty, the transactions in which it participates, and the context in which those transactions are carried out. The broader perspective allows counterparty risk to be assessed as a dynamic characteristic of a specific business relationship. Therefore, in this study, the counterparty is not considered in isolation but in relation to the operations, documents and the control environment.

Money laundering changes the nature of counterparty risk because the counterparty may be used not only as a contractual party but also as a vehicle for placement, layering or integration. For this reason, the assessment cannot be limited to solvency, delivery capacity or ordinary compliance reliability. In AML terms, the same counterparty characteristics acquire specific significance when they obscure beneficial ownership, disconnect transactions from the declared activity, create unexplained cross-border flows, involve higher-risk jurisdictions, sanctioned or offshore structures, nominee or trust arrangements,

unexplained third-party payments, unclear source of funds or adverse-media signals. The model therefore treats counterparty risk as AML-oriented counterparty risk, namely as the risk that the business relationship may be used to conceal the origin, movement, control or destination of funds, rather than only as a general business relationship risk.

The proposed approach allows counterparty risk to be considered as the result of the interaction between several groups of factors. The first group covers the identification characteristics, which include the completeness, reliability and verifiability of information about the counterparty. The second group refers to ownership and control. In this sense, the transparency of the structure, the possibility of identifying the beneficial owner and the presence of intermediary or representative relationships are taken into account. The third group concerns the economic activity, the sector, the scale of the activity, the business logic and the correspondence between activity and operations. The fourth covers transaction characteristics, with emphasis placed on the value, frequency, complexity, payment method and unusualness of the transactions. The fifth group refers to the behavior of the counterparty, such as the willingness to cooperate, the consistency of the data provided and the presence of contradictions. The three-factor matrix model systematizes risk factors and limits arbitrariness in their interpretation. It connects the established facts with the final risk profile and transforms qualitative information into an ordered evaluation logic. The model links the profile to the consequences for the due diligence, creates a documentary trail of the way the decision was formed and allows for reassessment when significant circumstances change. Therefore, the matrix has not only a classification but also a control function. The final risk profile in the proposed methodology is determined by a five-level classification: low, moderate, increased, high and critical risk. These categories are defined as a management guideline for the intensity of the due diligence, and should not be perceived as a mechanical result of an arbitrary point table. In this regard, for low risk, the verification can be standard if the specific circumstances are clear and verifiable. For moderate and increased risk, additional verification and clarification, more careful documentation and more active monitoring of the business relationship are required. For high and critical risk, enhanced due diligence, management judgment, effective management decision-making, stricter documentation and a clear decision on accepting, continuing or limiting the relationship are required. Therefore, a risk profile only has practical value if it is linked to specific follow-up actions.

The five groups of interacting features mentioned above are not treated as separate weighted variables. They are analytical subgroups that are operationalized through CE, TI and CV. Their relative importance depends on the fact pattern: beneficial ownership opacity and high-risk jurisdictional links usually affect CE most strongly; unusual value, frequency, third-party payment or lack of economic logic affect TI; missing source-of-funds evidence, contradictory documents or inability to verify sanctions, PEP or adverse-media information affect CV. In this initial framework, no fixed proportions are assigned to these five groups because such weights would require sectoral calibration and a larger empirical or expert-panel dataset.

The practical significance of the proposed methodology stems from the possibility of its application in real processes of acceptance, verification and periodic review of commercial counterparties and their relationships. The model uses information that is generally collected during the comprehensive examination. These are data on ownership, beneficial owner, activity, operations, documents and behavior in providing information. Therefore, its application does not require the development of a separate statistical system, but introduces a clear order for assessing already available or required data. The benefit for practice is that similar counterparties can be assessed according to the same logic, and different risk levels lead to different volumes of verification, monitoring and documentation. Thus, the methodology supports not only the classification of risk, but

also the defensibility of the subsequent decision in the face of internal control, audit or regulatory review. The dynamics of the business relationship also matter for the assessment. The risk profile is not a permanent characteristic of the counterparty, as it may change with new transactions, change of ownership, new beneficial owner, entry into a new sector, unusual payment behavior, contradictory data, refusal to cooperate, use of complex structures or links to jurisdictions with increased risk. Therefore, the matrix should not be applied as a one-off administrative form. It should be part of a cycle of assessment, documentation, monitoring and updating. Traceability is a fundamental requirement of internal control, as an assessment is only useful if it can be reconstructed. It is necessary to establish which facts were reported, how they were assessed, what risk profile was determined and what measures were taken. Without such traceability, the matrix would have limited value, because it would not allow verification of the relationship between the information and the decision. With a clear documentary trail, it becomes a tool for control, verification and protection of management judgment. The relationship between fact, assessment, decision and action is essential for the effective application of the risk-based approach. This relationship also underpins the proposed methodological framework.

The research gap addressed by the article is not the absence of AML risk factor lists but the insufficiently developed connection between qualitative counterparty information, a documented scoring logic and proportionate control consequences. Practical models often identify red flags and risk factors. Less often, they show how these factors are transformed into a final profile, how the profile determines the intensity of verification and how the transition from an established fact to a control decision is documented. The proposed model is therefore positioned as a structuring framework for internal control and management traceability, not as a predictive model for proving money laundering.

The methodological approach is based on four sequential steps: structuring the risk factors, assigning assessment values according to predefined scoring rules, aggregating the result and classifying it by initial managerial thresholds. Consistency in this study refers to procedural consistency and traceability of the assessment. It should not be interpreted as empirical proof that all independent assessors would necessarily assign identical scores, because inter-rater agreement is not tested in the present version.

The limitations of the model should be clearly acknowledged, as no matrix can capture all manifestations of risk. The scoring system does not replace case-by-case analysis, and the threshold classification does not eliminate the need for professional interpretation. The matrix should therefore be applied as a structuring framework, not as an automatic decision-making mechanism. It provides consistency without removing the context of the business relationship. The model creates comparability between assessments, but does not eliminate differences between specific cases. It supports control without exhausting the content of control activities.

The aim of the article is to propose a methodological framework for assessing the risk profile of commercial counterparties using a three-factor matrix model. The subject of the study is the relationship between risk factors, assessment values, threshold classification, due diligence measures and subsequent monitoring. The object of the study is the process of risk-based profiling of commercial counterparties in the context of measures against money laundering (Anti-Money Laundering, AML).

The main research thesis is that the three-factor matrix model can improve the structure, transparency and documentation of counterparty risk assessment when it is applied together with clear scoring rules, documentary evidence and review safeguards. This effect is achieved through four elements: identification of risk factors, assignment of assessment values, determination of a risk profile and linking of the profile to control actions. The contribution of the study is methodological and applied. It formulates a transparent

framework for structured risk profiling while explicitly refraining from claims of external validation, predictive accuracy or generalizability across all AML environments.

The structure of the article follows this logic. Section 2 reviews the literature and regulatory background on AML risk, due diligence, expert judgment and semi-quantitative matrix assessment. Section 3 presents the data sources, sample construction, scoring rules, aggregation logic, thresholds and limitations of the methodology. Section 4 applies the model to 25 anonymized counterparty profiles and links the scores to control measures. Section 5 discusses the methodological meaning of the results, including aggregation choices, threshold interpretation, AI-assisted monitoring and limitations. Section 6 summarizes the contribution and outlines directions for further empirical testing.

2. Literature Review

The scientific literature on anti-money laundering measures views risk as a multidimensional management category. It is not limited to the probability of a single adverse event occurring, but includes uncertainty, consequences, vulnerabilities and control conditions (Aven 2012, 2016). In the context of AML, risk arises from the interaction between an entity, property, economic activity, transaction, payment behavior, geographical environment and control infrastructure. Therefore, risk assessment requires not only customer identification, but also an analysis of the business relationship as an economic, legal and regulatory context. The basis of this approach, by examining money laundering as rational behavior, dependent on incentives, costs, sanctions and possibilities for concealment, is laid in the economic literature. It views the effectiveness of control as the result of a balance between regulatory burden, probability of detection and expected sanctions, and as a transnational process in which concealment techniques are adapted to the institutional and market environment (Masciandaro 1999; Levi and Reuter 2006). The global nature of the problem, the relationship between regulation and the behavior of actors, and the difficulty of quantifying the phenomenon have been emphasized in various other studies (Levi 2002; Buchanan 2004; Schneider and Windischbauer 2008; Chong and Lopez-de-Silanes 2015). These statements are of particular relevance to the present study because they shift attention from the formal identity of the customer to the broader risk context of his behavior and operations.

Critical studies on the effectiveness of AML regimes question the sufficiency of procedural compliance. The literature discusses the economic paradox between the high costs of AML control and the difficult-to-measure results, the risk of excessive mechanical reporting and the limited information value of signals (Geiger and Wünsch 2007; Harvey 2008; Chaikin 2009; Ferwerda 2009; Takáts 2011). It is also emphasized that effectiveness should be assessed not only through procedural indicators but also through actual control over criminal finances and predicate crimes (Pol 2018, 2020; Levi 2020). These dependencies, which are analyzed in the literature, show that any risk profile matrix should be evaluated not as a formal document but as a tool that leads to specific control actions.

The contemporary literature in the field of AML sets the risk-based approach as the main framework. In this sense, risk is not considered as a neutral technical quantity but as a category that depends on the institutional environment, legal and economic incentives, costs and the distribution of responsibilities between regulators and obliged entities (Demetis and Angell 2007; Dalla Pellegrina and Masciandaro 2009). The problem of correctly identifying low risk, the practical weaknesses of the risk-based approach and the coexistence of risk-based and rule-based procedures are separately highlighted (De Koker 2009; Simonova 2011; Ai 2012).

The analyzed literature outlines a clear methodological requirement, namely that the risk-based approach should allow for professional judgment, but this judgment needs to be comparable, documented and verifiable. If the assessment is entirely mechanical, it

may ignore the context. If it is completely free, it loses consistency. Matrix profiling is located between these two extremes. It structures professional judgment through risk factors, assessment values and thresholds, without replacing it with an automatic algorithm. The problem of uncertainty is particularly significant. In AML practice, reliable probabilities, complete information and a clear cause-and-effect relationship between an indicator and an outcome are often lacking, which is why a shift from a strictly risk-based approach to an approach that takes into account uncertainty is proposed (Bello and Harvey 2017). This is directly relevant for the assessment of commercial counterparties. Opaque ownership, unusual payment behavior, refusal to cooperate or complex transaction structure are not quantitative indicators in the strict sense. They are indicators that require interpretation. Therefore, the matrix should be presented as a semi-quantitative framework for structuring uncertainty and not as a model for precise mathematical measurement.

The developed scientific articles on expert judgment complement this perspective. The assessment of the risk resulting from money laundering is considered as a probabilistic judgment, in which the cognitive limitations of the assessors matter, and internal frames can both support and limit independent professional judgment (Ogbeide et al. 2023, 2025). Classic studies on inter-rater consistency are also significant because they show the need for expert classifications to be verifiable and reproducible (Cohen 1960; Fleiss 1971; Landis and Koch 1977). The indicated conclusions are key to the present study and play an essential role in the development of the model. The matrix should reduce arbitrariness but should not create the illusion of absolute objectivity. It disciplines the analysis but does not relieve the assessor from the need to interpret the specific case. Another group of studies considers the problem of money laundering as a networked, transnational, and adaptive process. Global money laundering flows, competition between jurisdictions to attract criminal funds, the role of private actors, financial surveillance and financial information sharing have been analyzed (Favarel-Garrigues et al. 2008, 2011; Unger and Rawlings 2008; Walker and Unger 2009; Helgesson and Mörtz 2019; Lagerwaard 2023; Lagerwaard and de Goede 2023). These developments show that AML risk is not only individual. It has a sectoral, institutional and jurisdictional dimension. All of the above supports the need for the matrix to include not only customer-related factors but also geographical, transactional, and behavioral factors. The relationship between AML control and due diligence is essential for the assessment of commercial counterparties. International good practices in customer due diligence, on the one hand, emphasize the importance of identification, beneficial ownership and ongoing monitoring. On the other hand, research on opaque companies shows why the difficulty of establishing beneficial ownership is a significant source of risk (Chitimira and Munedzi 2023; Sharman 2010; Allred et al. 2017). Techniques, typologies and practical mechanisms for concealing the origin or control of funds, as well as the situational approach to prevention, draw attention to opportunities where controls should limit the conditions for abuse (He 2010; Teichmann 2017; Levi 2015; Gilmour 2016). These sources support the thesis that the risk profile cannot be based on static data alone. It must take into account the behavior of the counterparty, the economic logic of the transactions and the dynamics of the business relationship.

The theoretical basis of the model is also supported by agency theory, information asymmetry theory and internal control/enterprise risk management. Agency theory explains why the interests and information of owners, managers, representatives and intermediaries may diverge, which is particularly important when beneficial ownership or effective control is opaque (Jensen and Meckling 1976). Information asymmetry theory explains why the obliged entity may not observe the true source of funds, the ultimate controller or the economic rationale of a transaction (Akerlof 1970). The COSO internal control and Enterprise Risk Management (ERM) frameworks support the process logic of the ma-

trix because they require risk identification, control activities, information, communication, monitoring and documentation (COSO 1992, 2004).

The literature on technological approaches to AML monitoring issues introduces a new perspective. Data visualization, relationship analysis, network analysis, machine learning, explainability and composite metrics can help detect suspicious activity and assess risk (Fronzetti Colladon and Remondi 2017; Chen et al. 2018; Singh and Best 2019; Kute et al. 2021; Gerbrands et al. 2022; Riccardi 2025). These studies show that risk can be modeled using multiple indicators but at the same time emphasize the need for automated decisions to be verifiable, explainable and subject to human control. This is essential for the present study because the three-factor matrix can function as an explainable layer between qualitative expert information and automated AML monitoring, without replacing professional judgment in borderline, incomplete, or critical cases.

Recent AML practice also shows that fintech, digital assets, instant payments and platform-based financial services increase the speed, fragmentation and cross-border character of transactions. These developments do not invalidate the risk-based approach, but they make counterparty assessment more dependent on reliable data integration, screening, monitoring, explainability and escalation rules. Professional AML surveys and industry reports also point to persistent challenges in alert backlogs, false positives, transaction-monitoring transformation and digital-asset AML risk (FATF 2021; PwC 2024; EY 2024; KPMG 2025). For this reason, the proposed matrix is positioned as an explainable layer that can connect KYC, UBO, sanctions, PEP, adverse-media and transaction-monitoring signals to a documented control response.

The literature review is complemented by empirical studies on the effectiveness and consequences of AML regulations. They examine AML policies and procedures in the banking sector, the relationship between AML regulations and financial inclusion, banking sector stability, compliance with AML procedures and quantitative approaches to assessing money laundering (Lokanan and Nasimi 2020; Ofoeda 2022; Durguti et al. 2023; Beebeejaun 2023; Ardizzi et al. 2014; Chong and Lopez-de-Silanes 2015). The aforementioned studies show that AML measures have a certain organizational cost. If the risk assessment is imprecise, it can lead to excessive control, withdrawal from client relationships due to risk, or inefficient allocation of resources. It follows that the matrix should be a proportional tool that distinguishes low, moderate, increased, high and critical risk, rather than mechanically increasing the level of control.

Industry-specific AML risk also matters. Banks, payment institutions, asset managers, virtual asset service providers, trade intermediaries and professional service providers do not face identical exposure. Sectoral differences influence the typical sources of funds, transaction velocity, use of intermediaries, delivery channels, geographic reach and quality of documentary evidence. The current model is designed as a general AML-oriented counterparty framework; sector-specific thresholds and weights should be calibrated in future studies.

The most recent research since 2022 draws attention to two additional specificities that are important for the current model. The first concerns the limitations of expert judgment and possible biases in internal AML assessments, which supports the need for clear criteria and a second review in borderline cases (Haffke 2023; Ogbeide et al. 2025). The second specificity examines the effect of AML measures, customer due diligence, virtual assets and sector risks through empirical data, emphasizing the importance of verifiable information, ongoing monitoring and proportionality of control actions (Aljassmi et al. 2024; Adaramola 2025; Meiryani 2024; Nazar et al. 2024; Andiojaya 2025). These studies strengthen the argument that the matrix model should be both applicable in practice and sufficiently cautious in interpreting the results.

The distinction between risk assessment and risk management is central. National risk assessments show that the mere existence of an assessment is not enough when there is no convincing order for identifying, comparing and prioritizing risks (Ferwerda and Reuter 2024). The literature reviewed highlights the need for better linking research directions, methods and practical applicability of results (Tiwari et al. 2020). Research on risk matrices is also important because it warns of possible problems with the incorrect use of assessment scales, thresholds and visual matrices (Cox 2008; Hubbard and Evans 2010; Duijm 2015; Peace 2017). The above conclusions can be transferred to the micro level. In the case of commercial counterparties, it is not enough to list risk factors. It is necessary to show how the factors are transformed into a profile, how the profile determines verification measures and how the result is updated over time.

The regulatory framework confirms the scientific conclusions drawn and indicated. The Financial Action Task Force (FATF) recommendations set a risk-based approach as the basis for identifying, assessing and understanding risks (FATF 2025), and the guidelines for the banking sector and those for professional services link the assessment to proportionate measures and internal controls (FATF 2014, 2019). The European Banking Authority's guidelines on risk factors for money laundering and terrorist financing highlight the link between the risk profile, the customer, the product, the service, the delivery channel and the geographical environment (European Banking Authority 2021). At the European Union level, the following are relevant: Regulation (EU) 2024/1624 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, Directive (EU) 2024/1640 on national mechanisms for the prevention of the use of the financial system for such purposes, and Regulation (EU) 2024/1620 establishing an Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA) (European Parliament and Council of the European Union 2024a, 2024b, 2024c). These instruments support the terminological choices in the study, including the concepts of obliged entity, customer due diligence, enhanced due diligence, beneficial owner and ongoing monitoring. In summary, the literature outlines several consistent points. First, AML risk is multidimensional and cannot be derived from customer identification alone. Second, the risk-based approach requires proportionality, but also methodological clarity. Third, professional judgment is inevitable, but must be structured through factors, indicators, values and thresholds. Fourth, the three-factor matrix model is suitable for qualitative, incomplete and contextual information, because it creates comparability and traceability. Fifth, the risk profile is only valuable if it is linked to due diligence, monitoring and updating measures.

On this basis, this study is positioned between four directions: risk-based AML control, due diligence, counterparty risk assessment and semi-quantitative matrix profiling. The contribution lies in the linking of risk factors, assessment value, threshold classification and control consequences in a single methodological framework. The three-factor matrix model is considered not as an administrative form but as a tool for internal control, management traceability and proportionate implementation of Anti-Money Laundering measures.

The three factors used in the model are not derived from statistical factor extraction. They are constructed by synthesizing three recurring dimensions in the literature and regulatory guidance: entity and ownership exposure, transaction behavior and verifiability or control conditions. This construction explains why the model is presented as a semi-quantitative assessment framework rather than as a predictive classifier. The link with the literature is therefore methodological: the framework translates risk-based AML logic into a documented sequence of factor identification, scoring, aggregation and control response.

3. Materials and Methods

In the scientific literature and in risk management practice, there are different approaches to identifying, assessing and controlling money laundering risk. However, when assessing commercial counterparties, there is often no single quantitative framework through which qualitative features can be translated into a clear and comparable risk score. This makes it difficult to compare individual counterparties, document the assessment and justify different volumes of subsequent control actions.

This study proposes a three-factor matrix model for structuring and documenting the risk profile of commercial counterparties in the context of AML measures. The model is designed to assess already established risk features. It is not a statistical detection model and does not aim to prove the presence of money laundering. Its task is to transform information about the counterparty, operations and data verifiability into an ordered risk score that can guide due diligence, monitoring, escalation and documentation. The resulting score is therefore a management classification tool, not evidence of illegal conduct.

The study is methodological and applied in nature. It does not test a statistical hypothesis on a representative sample but develops and applies an assessment algorithm to 25 anonymized counterparty profiles. The profiles were selected purposively to cover different combinations of counterparty exposure, transaction impact and control vulnerability. The approach is justified by the specifics of AML risk, where many relevant indicators are qualitative and contextual: unclear ownership, difficulty in establishing a beneficial owner, unusual payment behavior, contradictory documents, refusal to cooperate, links to higher-risk jurisdictions or inconsistency between declared activity and actual operations. These indicators are difficult to measure through classical statistical methods in a small confidential dataset, but they can be assessed through a clear rubric and documented professional judgment.

The methodological basis of the study includes three directions. The first is related to risk assessment, internal control, documentation and monitoring, which form the process logic of the model. The second direction is related to the three-factor matrix determination of a risk profile and justifies the use of a five-point scale, a formula for overall risk and rating interpretation. The third direction includes scientific and regulatory sources on the risk-based approach, due diligence, beneficial ownership, monitoring and proportionality of measures against money laundering (AML). Counterparty profiles are presented as summarized assessment cases. They do not contain personal data, bank transactions, identifying documents or confidential commercial information that would allow the recognition of a specific person or organization. The unit of analysis is the commercial counterparty within a specific business relationship. The counterparty is not assessed only as a legal entity but through its participation in a specific economic relationship. The analysis covers legal status, representation, ownership structure, beneficial owner, sector of activity, nature of operations, payment method, geographical connections, documentary security and behavior in providing information. Risk may arise not only from the person, but also from the operation, payment mechanism, lack of transparency or the inability to verify the information provided.

Data Sources, Sample Construction and Anonymization

The empirical material consists of 25 anonymized counterparty assessment profiles generated in 2026 within commercial counterparty review procedures. The profiles do not contain personal data, bank account identifiers, names of legal entities, identifying documents or confidential commercial information. Anonymization was performed by removing identifiers and preserving only the risk-relevant characteristics required for methodological demonstration.

The underlying evidence categories included registration and corporate documents, ownership and beneficial ownership information, representation data, contracts, invoices or payment terms, available transaction information, external register checks, sanctions, politically exposed person and adverse-media screening results, information requests and internal review notes. The demonstration did not use confidential bank transaction records and did not reconstruct a complete time series for all profiles. Where historical transaction information was available in the counterparty file, it was used only to assess value, frequency, payment method and economic logic within the transaction impact factor.

The sample was purposive and illustrative. It was not designed to estimate the frequency of AML risk levels in a market, sector, jurisdiction or institution. The labels K1–K25 preserve the order of case processing and have no classificatory significance. For this reason, the analysis demonstrates the model’s application logic and traceability, but it does not establish predictive accuracy or external validity.

The selection of the 25 profiles was therefore based on AML relevance rather than ordinary commercial representativeness. The set includes cases with variations in beneficial ownership transparency, ownership chains, sector vulnerability, cross-border or higher-risk geographical links, source-of-funds clarity, third-party or intermediary involvement, payment characteristics, document completeness and verification behavior. Exact countries, sectors and identifying combinations are not disclosed because such information could make individual cases indirectly recognizable.

The three-factor matrix model uses three main factors: counterparty exposure, transaction impact and control vulnerability. Counterparty exposure measures the risk associated with the counterparty itself and the environment in which it operates. Transaction impact measures the risk associated with the nature, value, frequency, payment method and economic logic of the operations. Control vulnerability measures the risk associated with the limited ability to verify, document and manage information. The three factors cover the main questions in the AML assessment: who the counterparty is, what operations it carries out and to what extent the information about it can be verified.

To make the AML link explicit, CE includes entity, ownership, beneficial ownership, sectoral and jurisdictional indicators; TI includes transaction value, frequency, source and movement of funds, third-party involvement and economic logic; CV includes the ability to verify UBO, source-of-funds/source-of-wealth evidence, sanctions, PEP, adverse-media screening and document consistency. Thus, the model does not assess counterparty risk in an unrestricted commercial sense, but only the features relevant for AML due diligence and ongoing monitoring.

To ensure consistent and reproducible assessment of counterparty risk, Table 1 presents the three-factor matrix for assessing counterparty AML risk. It combines the three main factors of the model—counterparty exposure, transaction impact and control vulnerability—and relates them to a five-point rating scale. The scale starts at 1, not 0, because every business relationship contains a minimum baseline level of risk. A value of 1 indicates minimal risk, where information is clear and verifiable, and a value of 5 indicates critical risk, where key prerequisites for reliable assessment or control are missing.

Table 1. Three-factor matrix for assessing counterparty AML risk.

Scale Level	Counterparty Exposure (CE)	Transaction Impact (TI)	Control Vulnerability (CV)
1	The counterparty is identified; ownership is clear; the beneficial owner is established; the sector and geographical links do not pose significant risks.	The operations are standard, with common value, low complexity and clear economic logic.	The information is complete, consistent and verifiable; the documents are available and correspond to the circumstances stated.

2	There are limited specificities in the structure, representation or sector that are explainable, documented and do not significantly hinder the assessment.	The operations have distinct characteristics, but correspond to the activity and do not require significant additional clarification.	Limited documentary gaps were identified, which have been addressed or can be easily verified.
3	There are indications that require further clarification, including intermediate ownership, specific sector, representation through a third party or additional geographical connection. AML-specific examples include additional UBO documentation, nominee or intermediary links and preliminary adverse-media indications.	Any unusual value, frequency, payment method, or level of transaction complexity requires additional verification. AML-specific examples include atypical frequency, third-party payment involvement or source-of-funds questions.	Some of the information requires completion; verifiability is possible but not immediate. Verification should include UBO, source-of-funds, sanctions, PEP and adverse-media evidence where relevant.
4	There is a complex structure, significant sectoral vulnerability, representation through intermediaries, significant geographical connections or difficulty in establishing control. AML-specific examples include multi-tiered ownership chains, offshore links, high-risk jurisdictions, trusts or nominee arrangements.	There are complex, unusual or difficult to explain operations; a significant discrepancy between an activity and a transaction is identified. AML-specific examples include unexplained cross-border flows, layering-like movement or mismatch between invoice, payment account and activity.	There are contradictions, delays, incomplete documents, limited verifiability, or inconsistent explanations. Contradictions in UBO, source-of-funds or screening results increase this factor.
5	The effective control, beneficial ownership or economic profile of the counterparty cannot be reliably established. AML-specific examples include an unidentifiable UBO, sanctioned or high-risk jurisdictional links and unresolved adverse-media or PEP concerns.	There are operations without clear economic logic, significant opacity or a high-risk payment model. AML-specific examples include transactions without credible source of funds, opaque third-party payments or patterns consistent with layering.	There is a denial of key information, an inability to verify, or significant inconsistencies that prevent a reliable assessment. Inability to verify UBO, source of funds, sanctions/PEP/adverse-media status or key transaction evidence prevents reliable AML assessment.

Source: Prepared by authors.

To reduce assessor discretion, the five-point scale should be applied together with the operational scoring rubric in Table 2. The rubric does not remove professional judgment but requires that each score be linked to observable facts, documentary evidence and a written rationale.

Table 2. Operational scoring rubric for applying the five-point scale.

Assessment Situation	Operational Scoring Rule	Documentation Requirement	Control Safeguard
Single dominant risk feature within one factor	Assign the level corresponding to the most significant documented feature, rather than averaging contradictory indicators.	Record the feature, source document and reason for the assigned level.	Second review is recommended when the assigned level moves the profile to increased, high or critical risk.
Several weaker indicators within one factor	The score may be increased by one level when several weaker indicators cumulate.	Explain the cumulative effect and specify why the increase is proportionate.	The increase cannot be automatic; it requires written justification.

	tively reduce transparency or verifiability.		
Missing key evidence	Absence of essential evidence is not treated as low risk; it normally increases control vulnerability and may also affect exposure or transaction impact.	Identify the missing evidence and the unsuccessful verification steps.	Escalation is required when the missing evidence concerns beneficial ownership, source of funds or economic logic.
Borderline between two levels	Where uncertainty remains unresolved, the higher level is used if the ambiguity affects ownership, transaction logic or verifiability.	Document the unresolved issue and the reason for conservative classification.	Borderline increased, high and critical profiles should be reviewed by a competent second person or control function.
Contradictory information	Contradictions are reflected primarily in control vulnerability and, where relevant, also in exposure or transaction impact.	State the contradiction and the documents or explanations that conflict.	A relationship should not be approved routinely while material contradictions remain unresolved.
Mitigating evidence	A lower level may be assigned only when mitigating evidence is independent, current and verifiable.	Record the mitigating source and why it neutralizes or reduces the risk feature.	Self-declarations alone should not reduce the score when independent verification is available but absent.
AML-specific indicator mapping	When a FATF-style indicator is present, such as high-risk jurisdiction, nominee ownership, complex UBO chain, unexplained third-party payment, unclear source of funds, PEP/sanctions/adverse-media signal or digital-asset exposure, the indicator is assigned to CE, TI or CV according to its substantive meaning.	Record the indicator, the source of evidence and the affected factor. The rationale should explain why the indicator increases the AML-oriented risk score.	Where such an indicator affects more than one factor, the overlap must be explained and a second review is recommended for increased, high and critical profiles.

Source: Prepared by authors.

Counterparty exposure is determined on the basis of documented data on legal status, registration, representation, ownership, beneficial owner, sector and geographical links. The source of the score must be stated in the assessment file. This factor is not limited to formal identification. A counterparty with complete registration data may still have high exposure if the beneficial owner is difficult to determine, the ownership is opaque or the structure lacks convincing economic logic.

Transaction impact is determined on the basis of available information on the type, value, frequency, payment method, source of funds and economic logic of the operations. Where time-series transaction data are available, they may support the assessment of frequency and deviation from the expected profile. In the present anonymized application, the model uses the transaction information preserved in the counterparty files and does not perform a statistical time-series analysis.

Control vulnerability is determined on the basis of document quality, consistency of explanations, willingness to cooperate and possibility of independent verification. This factor is independent because AML risk depends not only on the counterparty and operations, but also on whether the obliged entity can verify and document the relevant cir-

cumstances. Incomplete, contradictory or unavailable information should not lead to an artificially low assessment. It is treated as a vulnerability of the control environment and must be explicitly recorded.

The overall risk score is determined by the product of the three main factors:

$$\text{Overall Risk Score (ORS)} = \text{Counterparty Exposure (CE)} \times \text{Transaction Impact (TI)} \times \text{Control Vulnerability (CV)}$$

Each factor takes a value from 1 to 5, which allows a uniform assessment logic for all profiles. The minimum score is 1 when all three factors are rated 1. The maximum score is 125 when all factors are rated 5.

The product is used as an initial conservative aggregation rule because the three factors may reinforce each other when exposure, transaction impact and control vulnerability increase simultaneously. The study does not claim that multiplication is empirically superior to additive, weighted, fuzzy-logic, analytic hierarchy process or data-driven alternatives. Rather, multiplication is used to prevent cases with simultaneous high values across all three dimensions from being diluted by lower values on a single dimension. The result is interpreted as a classification guide and not as an exact statistical measure (Cox 2008; Hubbard and Evans 2010; Duijm 2015; Peace 2017). The formula does not predict money laundering and does not prove wrongdoing. It creates a documented and comparable transformation of qualitative risk features into a risk category that can be linked to control actions.

The initial version of the model does not introduce preliminary weights between the three factors. This choice is conservative because reliable weights would require a larger empirical dataset, an expert panel or calibration against external AML outcomes. Equal starting treatment of the three factors does not mean that they have identical factual importance in every case. It means that differences in importance are first reflected in the assigned factor levels and only later, in future research, may be refined through weighting or multi-criteria decision-making procedures (Saaty 2008). Table 3 summarizes the main aggregation alternatives considered and explains why the present article adopts multiplication as a transparent first-stage rule rather than a statistically optimized rule.

Table 3. Aggregation alternatives considered in relation to the proposed model.

Aggregation Approach	Potential Advantage	Limitation in the Present Study	Treatment in This Article
Additive score	Simple and transparent; easy to audit.	May dilute simultaneous high values across CE, TI and CV.	Used only as a comparison point; not selected as the main rule.
Weighted score	Can reflect different empirical or expert importance of factors.	Requires defensible weights derived from a larger sample, expert panel or external outcomes.	Reserved for future calibration.
Analytic Hierarchy Process (AHP) or other multi-criteria methods	Useful when pairwise expert comparisons are available.	Would require a structured expert elicitation stage beyond the present dataset.	Recognized as a future refinement.
Fuzzy-logic approach	Can handle gradual membership and ambiguity.	Requires additional membership functions and validation that are not available here.	Recognized as a future refinement.
Predictive or statistical model	Can estimate observed outcomes if labeled data are available.	No external labels, Suspicious Activity Report (SAR)/Suspicious Transaction Report (STR) outcomes	Not claimed in this article.

		or regulatory findings are available for the anonymized profiles.	
Multiplicative ORS	Preserves transparency and emphasizes simultaneous accumulation across the three factors.	Initial managerial rule; not externally validated as empirically superior.	Adopted as the first-stage semi-quantitative rule.

Source: Prepared by authors.

The five-point scale in the model should be understood as an ordered rating scale, not as a continuous mathematical quantity. Therefore, the thresholds are initial managerial thresholds. They are based on the achievable values produced by the formula and are used to ensure that similar profiles are treated by the same internal logic. They are not presented as empirically observed AML outcome thresholds. The distinction between adjacent categories should therefore be interpreted together with the underlying factor configuration and documented facts, not mechanically from the numerical score alone.

After determining the values for the three factors, the ORS is compared with predefined managerial risk limits. These limits are not statistically derived from observed AML outcomes. They arise from the construction of the model and from the limited set of values achievable when three integer scores from 1 to 5 are multiplied. Table 4 shows how these values are grouped into five risk levels for internal control purposes.

Table 4. Risk level limits according to the ORS value.

ORS Range	Achievable ORS Values in the Range	Risk Level	Justification of the Border
1–20	1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 16, 18, 20	Low risk	Low overall accumulation. Standard inspection and routine monitoring are sufficient.
21–40	24, 25, 27, 30, 32, 36, 40	Moderate risk	The first achievable value after 20 is 24. Additional documents and further clarification are required.
41–70	45, 48, 50, 60, 64	Increased risk	Values of 45 and above indicate more pronounced accumulation. Further investigation is required.
71–99	75, 80	High risk	It is reached when two or three factors are high. Extensive verification and management decisions are required.
100–125	100, 125	Critical risk	100 and 125 indicate two or three maximum values. Special management review or denial is required.

Source: Prepared by authors.

Table 4 defines the initial managerial limits of risk levels according to the ORS value. Since the result is obtained by multiplying three integer scores from 1 to 5, not all numbers between 1 and 125 are possible. The first value above low risk is 24; the first value above moderate risk is 45; the next transition is to 75; and critical risk begins at 100 because this value is reached with two maximum scores and one high score. These limits make the classification transparent and auditable, but they do not prove that a score of 45 represents an empirically different AML outcome from a score of 40. For this reason, the score must be interpreted together with the documented facts and factor configuration.

To limit subjectivity, the methodology requires that each assigned value be linked to established facts, documentary evidence and a written rationale. Borderline cases between two risk levels should be explicitly justified. Increased, high and critical profiles should be subject to second internal review by a competent person or control function when such review is available. The present study does not calculate Cohen's kappa, Fleiss' kappa or another inter-rater agreement indicator because the 25 profiles were not independently

scored by multiple assessors. Accordingly, reproducibility is used in the limited sense of procedural traceability, while empirical assessor agreement remains a necessary direction for future research (Cohen 1960; Fleiss 1971; Landis and Koch 1977).

When determining the final profile, all identified features with high AML significance are included in the assessment of the three factors before calculating the overall risk score. The inability to identify a beneficial owner, refusal to provide key information, contradictory documents regarding the ownership or origin of funds, as well as operations without a clear economic logic, increase the values of the relevant factors. Most often, these features are reflected in the control vulnerability, but if necessary they also affect the counterparty exposure or transaction impact. Thus, the model retains its three-factor structure and avoids the introduction of an additional element after the formula. The final risk level is derived from the overall risk score and the rating scale, and subsequent measures are determined according to the established profile.

Signs of high AML significance are included in the quantitative assessment through the relevant factor and are not added as a separate adjustment after the ORS calculation. Denial of key information and contradictory documents increase control vulnerability because they limit the possibility of reliable verification. Unclear ownership or difficulty in establishing de facto control are reflected in the counterparty exposure. Operations without a convincing economic logic or involvement of third parties without a clear justification are reflected in the transaction impact. Thus, the overall risk score remains the carrier of all significant risk signs within the three-factor structure.

Algorithm for applying the methodology

The logic of the three-factor matrix model is presented in Figure 1 as a four-step process with an update cycle. The scheme reproduces the practical sequence of the assessment: identification and verification of the information base; assignment of values for CE, TI and CV; calculation of ORS; control checking for critical features; and determination of a final risk profile with an appropriate control response.

Figure 1 shows that the assessment begins with the collection and verification of information about the counterparty, ownership, activity, operations and documents. The established facts are then converted into CE, TI and CV values, and the overall score is calculated using $ORS = CE \times TI \times CV$. Before the final classification, a control check is performed for signs that may limit the reliability of the assessment: refusal to provide information, unidentifiable beneficial owner, contradictory documents or operations without a clear economic logic. The final output of the algorithm is a risk profile associated with due diligence, monitoring, escalation, limitation or denial.

The update cycle shows that the risk profile reflects the state of the business relationship at the time of the assessment. A change in ownership, beneficial owner, effective control, operations, geographical links, documents or verification behavior returns the process to the first stage and requires re-application of the matrix. In an automated AML environment, the same logic can be used as a workflow with triggers, review tasks and subsequent human control at increased, high or critical risk.

The limitations of the methodology should be taken into account when applying it. The testing on 25 counterparty profiles demonstrates the applicability, internal logic and usefulness of the model for risk management, but does not constitute a statistical test on a representative sample. Due to the limited scope of the profiles, no indicators of incorrect over- or under-classifications are calculated at this stage. The result depends on the quality of the input information, the consistent application of the criteria and the documentation of the grounds for the assessment. The thresholds may be refined in future application to a larger sample of counterparties. The matrix cannot cover all risk scenarios; therefore,

professional judgment remains necessary in borderline cases, complex structures and incomplete information.

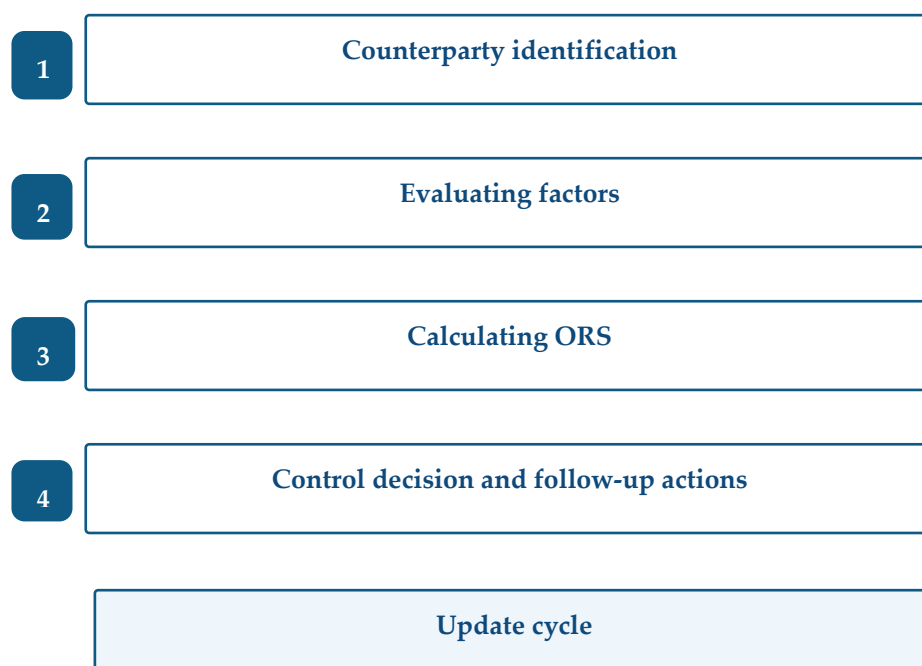


Figure 1. Algorithm for applying the three-factor matrix model in assessing counterparty AML risk. Source: Prepared by authors.

Documentation is a mandatory part of the methodology. Each assessment should contain data on the information used, the values assigned to the three factors, the overall risk score, the risk level determined and the chosen follow-up actions. Where there are indications of high AML significance, these should be reflected in the rationale for the values for the relevant factors. The documentary trail should allow for the reconstruction of the decision. An external reviewer should be able to trace how a specific risk profile was reached from specific facts.

Procedural reproducibility does not mean complete identity of expert judgment. It means that different evaluators, using the same information and the same methodology, should be able to reconstruct the assessment path and explain the reasons for any difference in scoring. In the present article, this remains a design objective of the methodology rather than an empirically tested property. Empirical reliability requires an additional inter-rater study with independent assessors and an appropriate agreement statistic.

The specified limitations determine the conditions for the correct use of the three-factor matrix model. The methodology should be understood as a tool for structuring a quantitative assessment and not as an automatic decision-making mechanism. Its value lies in the fact that it turns the assessment of counterparty AML risk into a consistent process with clear grounds and the possibility of updating. When properly applied, the matrix allows for better traceability of decisions and more proportionate risk management. This function is central to the practical application presented in the next section.

4. Results

The practical application of the proposed three-factor matrix model was carried out on 25 anonymized profiles of commercial counterparties, designated as K1–K25. The analysis was conducted in 2026 and covers different levels of complexity, transparency, economic logic and verifiability. Each profile was assessed using the same matrix, which allows the application logic to be demonstrated in a comparable way. The application has a methodological function: it shows how the model works in an assessment procedure, without presenting the results as proof of correct AML outcomes or as a statistical test on a representative sample.

4.1. Scope and Procedure of the Application

The testing array includes 25 anonymized profiles with different risk configurations. The profiles were not arranged according to a predefined risk level. The numbering K1–K25 follows the order of case processing and has no classification significance. The selection has a purposive applied nature: cases were selected to demonstrate the behavior of the model under various combinations of CE, TI and CV. The procedure follows the same order for all profiles: systematization of information, assessment by the three factors, calculation of ORS and comparison with the managerial rating scale. All high-significance AML indicators are included in the three factors before the overall score is calculated.

Specific country names, exact industries and identifying combinations of sector, jurisdiction and transaction pattern are not disclosed. This limitation follows from the confidentiality of the underlying files and the small size of the demonstration set, where granular sector–jurisdiction combinations could enable re-identification. For this reason, Table 5 reports only risk-relevant generalized categories rather than exact jurisdictions or industry labels.

Table 5. Characteristics of the assessed counterparty profiles.

Profile	Type of Business Relationship	Leading Feature
K1	Local supplier of standard goods	Clear ownership, established beneficial owner and complete documentation.
K2	Counterparty with intermediate ownership	Ownership is explained, but verification requires additional documents.
K3	Counterparty in a sector with higher AML vulnerability	Sector risk and documentary restrictions increase the overall result. AML-specific indicator: sector vulnerability combined with restricted documentary evidence.
K4	Counterparty with medium frequency of operations	Operations are more frequent, but the economic logic is clear.
K5	Counterparty with significant payments	High transaction impact necessitates extended verification. AML-specific indicator: higher transaction value requiring source-of-funds and economic-purpose verification.
K6	Service provider with a typical contractual structure	Low exposure and verifiable information with limited documentary clarification.
K7	Counterparty with operations without clear economic logic	All three factors reach their maximum value due to a combination of opacity, unexplained operations, and limited verifiability. AML-specific indicator: opacity, unexplained operations and unverifiable information create a layering-oriented concern.
K8	Specialized service provider	Average values for the three factors and need for further clarification.
K9	Commercial intermediary with complicated ownership	Verifiability is limited for significant operations and complex structure. AML-specific indicator: complex ownership and limited verifiability may obscure beneficial ownership and control.

K10	Local supplier with regular deliveries	Standard operations, but some of the documents require completion.
K11	Counterparty with the participation of an intermediary	The operations are significant, and verification requires additional evidence.
K12	Foreign supplier with verifiable structure	The cross-border element requires external references and additional verification. AML-specific indicator: cross-border exposure requires jurisdictional, sanctions/PEP and adverse-media checks.
K13	Counterparty with difficulty establishing control	The strongest risk stems from ownership and de facto control.
K14	Supplier with separate documentary features	There is no refusal to cooperate, and gaps can be addressed.
K15	Counterparty with unidentifiable beneficial owner	Basic conditions for reliable verification of the beneficial owner are missing. AML-specific indicator: inability to establish the UBO prevents reliable AML due diligence.
K16	Foreign trading partner	Increased value of operations and more difficult verifiability. AML-specific indicator: increased transaction value and limited verifiability require source-of-funds review.
K17	Partner with a cross-border structure	Simultaneously high values for all three factors, without reaching maximum opacity. AML-specific indicator: cross-border structure, high factor values and control vulnerability require enhanced review.
K18	Counterparty with a cross-border element and verifiable ownership	Geographical connections require external references, but the structure remains traceable.
K19	Counterparty with complex ownership and significant operations	The combination of exposure and control vulnerability is high. AML-specific indicator: complex ownership, significant operations and high control vulnerability affect UBO and source-of-funds reliability.
K20	Counterparty with more significant operations	The operations are significant and the verifiability is limited in the initial stage.
K21	Counterparty with key information refusal	The refusal is reflected in the control-vulnerability score, and the operations remain unexplained. AML-specific indicator: refusal of key information and unexplained operations require escalation.
K22	Supplier with a typical contractual structure	The operations are common and economically explainable with sufficient verifiable information.
K23	Counterparty with conflicting ownership documents	The contradictions concern ownership, operations, and verifiability. AML-specific indicator: contradictory ownership documents and transaction inconsistency prevent routine approval.
K24	Counterparty with a complex contractual structure	Exposure and control vulnerability are increased, although operations remain explainable.
K25	Supplier with limited documentary specifications	There are limited gaps that can be checked and fixed.

Source: Prepared by authors.

The generalized profiles were selected because they contain AML-relevant configurations rather than ordinary procurement or logistics risk alone. The profile descriptions were therefore revised to indicate the AML logic behind the assessment: beneficial ownership opacity, source-of-funds uncertainty, jurisdictional exposure, intermediary or third-party involvement, transaction inconsistency and control vulnerability.

4.2. Profiles of the Rated Counterparties

Table 5 organizes the 25 counterparty profiles by a brief description of the business relationship and the leading risk characteristic. The descriptions indicate the factual basis from which the CE, TI and CV values are derived. The profiles are presented in the order of case processing, not in ascending or descending risk value.

4.3. Quantitative Assessment of the 25 Profiles

After systematizing the qualitative features, the five-point rating scale was applied for the three factors. Table 6 presents the assigned values, the total risk score, and the risk level according to the rating scale. The data in it are limited to the indicators that have independent analytical value: CE, TI, CV, ORS and risk level. The profiles are preserved in the order of processing, and are not arranged by score, so as not to create the impression of a pre-constructed distribution.

Table 6. Quantitative assessment using the three-factor matrix model.

Profile	CE	TI	CV	ORS	Risk Level
K1	1	2	1	2	Low risk
K2	3	3	4	36	Moderate risk
K3	4	3	5	60	Increased risk
K4	2	3	3	18	Low risk
K5	4	5	4	80	High risk
K6	2	2	3	12	Low risk
K7	5	5	5	125	Critical risk
K8	3	3	3	27	Moderate risk
K9	4	4	5	80	High risk
K10	1	2	3	6	Low risk
K11	3	5	5	75	High risk
K12	4	3	4	48	Increased risk
K13	5	4	4	80	High risk
K14	2	3	4	24	Moderate risk
K15	5	5	4	100	Critical risk
K16	3	4	5	60	Increased risk
K17	4	4	4	64	Increased risk
K18	4	3	3	36	Moderate risk
K19	5	4	5	100	Critical risk
K20	2	4	5	40	Moderate risk
K21	5	5	5	125	Critical risk
K22	2	3	3	18	Low risk
K23	4	5	5	100	Critical risk
K24	3	4	4	48	Increased risk
K25	2	2	3	12	Low risk

Source: Prepared by authors.

The data in Table 6 are important not as evidence that the model produces correct AML outcomes but as an audit trail for the way in which professional judgment is translated into a structured classification. The array contains six low-risk profiles, five moderate-risk profiles, five increased-risk profiles, four high-risk profiles and five critical-risk profiles. This distribution shows the behavior of the model for different combinations of CE, TI and CV, without implying that the profiles are representative of a wider market or sector. From an internal control perspective, the same ORS value can result from different factor configurations. Therefore, the final number should be interpreted together with the specific grounds for the assessment, not separately from them.

4.4. Three-Dimensional Visualization and Aggregation Sensitivity

Figure 2 visualizes the same assessment results in a three-dimensional space where the axes represent CE, TI and CV. The visualization clarifies that the risk level is not only a function of a final number but also of the configuration of the three underlying factors. It also shows why profiles with similar ORS values may require different documentation and review, depending on whether the score is driven by exposure, transaction characteristics or control vulnerability.

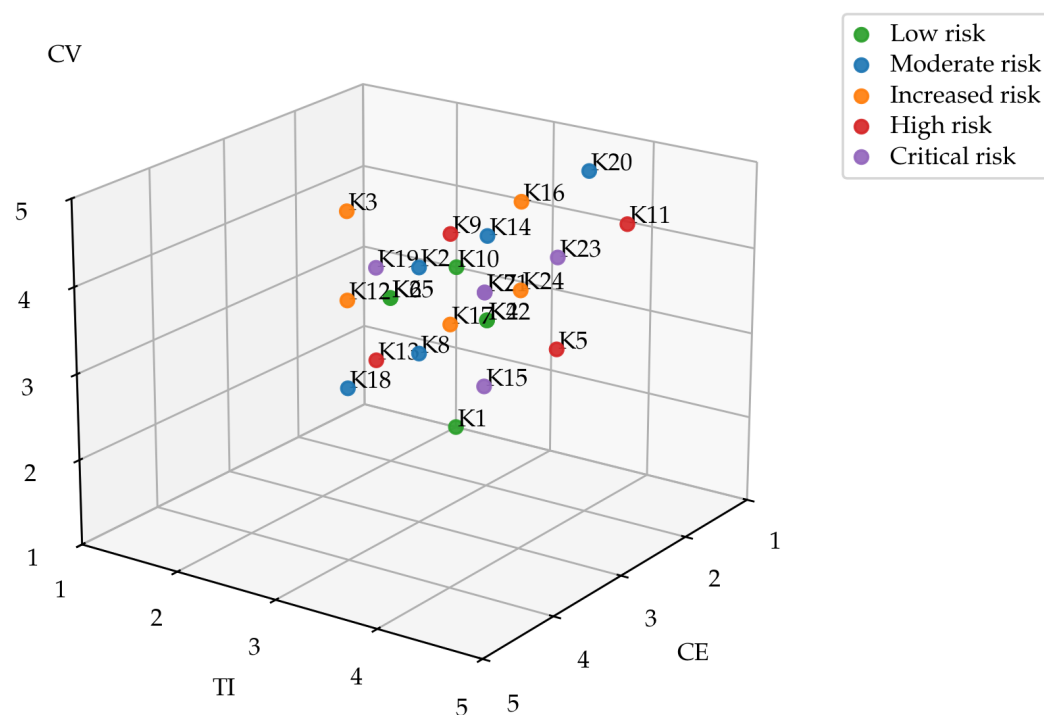


Figure 2. Three-dimensional visualization of the 25 counterparty profiles by CE, TI and CV. Source: Prepared by authors.

As an exploratory sensitivity check, the ranking produced by ORS was compared with the simple additive score $CE + TI + CV$ for the same 25 profiles. The rank association is high (Spearman's $\rho = 0.997$), which indicates that the multiplicative rule does not create a contradictory ordering of the profiles. Its main methodological effect is stronger separation of cases in which all three dimensions are simultaneously high. This check does not validate the model against external AML outcomes; it only shows that the proposed aggregation is internally coherent within the demonstration dataset.

4.5. Recommended Control Measures

The practical value of the methodology is manifested through the relationship between the risk level and subsequent actions. Table 7 presents recommended measures by risk levels. The measures are derived from the risk-based approach, proportional due diligence logic, internal control requirements and the need for escalation where verifiability is limited. They are not presented as empirically proven measures for reducing observed money-laundering outcomes. Table 7 has a synthesizing function: it does not replace expert judgment on the specific profile but determines the minimum control response that follows from the corresponding ORS range.

Table 7. Recommended control measures by risk level.

Risk Level	Recommended Control Measures
Low risk	Standard due diligence; documentation of basic identification information, ownership, beneficial owner and contractual basis; update upon significant change. AML-specific minimum: standard Customer Due Diligence (CDD), UBO confirmation, sanctions/PEP/adverse-media screening and update upon ownership or activity change.
Moderate risk	Additional clarification of individual circumstances; completion of missing or incomplete documents; more careful ongoing monitoring until verifiability is confirmed. AML-specific measures: targeted clarification of UBO, source of funds and jurisdictional exposure; completion of missing screening evidence.
Increased risk	Extensive verification of ownership, beneficial owner, source of funds, economic logic of operations and jurisdictional connections; documentation of the grounds for continuing the relationship. AML-specific measures: enhanced due diligence, source-of-funds/source-of-wealth verification, review of high-risk jurisdictions, intermediary roles and adverse-media indicators.
High risk	Enhanced due diligence; second internal review or management decision; extended documentation; explicit decision to accept, continue, limit or terminate. AML-specific measures: MLRO or senior-management review, enhanced monitoring, documented decision on acceptance or continuation, and internal assessment of whether suspicious-activity escalation is required.
Critical risk	Denial, termination or special management review when the risk cannot be reliably clarified; non-admission of standard approval in case of residual opacity. AML-specific measures: refusal, termination or special management review where residual opacity remains; standard approval is excluded and internal reporting assessment should be documented where suspicion is identified.

Source: Prepared by authors.

Table 7 shows that the risk classification has direct managerial significance. At low risk, control remains standard because the information is clear and verifiable. At moderate and increased risk, additional evidence, more active monitoring and clearer documentation of the grounds for the assessment are required. At high and critical risk, the decision cannot remain only at the operational level, as it affects the acceptance, continuation, limitation or termination of the business relationship.

4.6. Application Summary

The practical application on 25 counterparty profiles demonstrates the applicability of the 3-factor matrix model in an assessment procedure. The obtained values are consistent with the expected logic of the model: risk increases with simultaneous increases in CE, TI and CV. The profile-oriented control measures and the three-dimensional visualization show how the quantitative result can be transformed into a differentiated control response. These findings should be interpreted as evidence of procedural applicability and traceability, not as evidence of predictive accuracy or external validation.

5. Discussion

The application to 25 anonymized counterparty profiles shows that the 3-factor matrix model can serve as a tool for structured assessment of counterparty AML risk. Its main value is not the production of a definitive truth about money laundering but the documented relationship between factual information, assigned factor values, risk level and subsequent measures. In risk, audit and internal control practice, this relationship is crucial because the assessment must be explainable, reviewable and proportionate. The

model therefore reduces unstructured discretion, but it does not eliminate professional judgment or the need for second review in borderline and high-risk cases.

The choice of multiplication instead of addition should be interpreted cautiously. It has methodological significance as a transparent first-stage rule for simultaneous accumulation across CE, TI and CV, but it is not presented as an empirically superior aggregation function. Additive, weighted, AHP-based and fuzzy-logic alternatives may be appropriate where larger datasets, expert panels or external benchmarks are available. The present contribution is therefore narrower: it shows how a conservative multiplicative rule can be used and documented consistently in an applied AML risk-assessment procedure.

The limits of the rating scale should be understood as managerial thresholds, not as statistically proven AML outcome boundaries. They are aligned with the values that can actually be obtained from $ORS = CE \times TI \times CV$ and make the classification auditable. However, the transition from 40 to 45 should not be interpreted mechanically as proof of a materially different real-world AML outcome. It should trigger a review of the underlying configuration, the factual basis and the control response attached to the category.

The three-factor model differs from the classic two-factor matrices, which usually combine probability and impact. In AML risk, probability often cannot be reliably measured because information is incomplete, counterparty behavior is adaptive, and the relationship between an indicator and actual risk is not always direct. Therefore, the verifiability of information has an independent meaning. Control vulnerability is not an added fourth element, but one of the three main factors. It shows the extent to which the obligated entity can verify ownership, operations, documents and the origin of funds. Without this factor, the model would underestimate cases where there is only superficial data, but its reliability is limited.

The methodology has practical value because it can support the acceptance of new counterparties, periodic review and extraordinary update in case of changing circumstances. It allows an obliged entity to justify why one profile requires standard due diligence, whereas another requires enhanced due diligence, a management decision, or refusal. Linking the resulting profile to specific control measures is particularly important for internal control, because the assessment must be not only correct, but also verifiable. At the same time, the model does not prove money laundering and should not be used as a tool for detecting a violation. Its function is to classify the risk, direct the appropriate measures and create a documentary trail for subsequent verification.

The purpose of the quantitative criterion is therefore not to predict money laundering and not to establish evidence of illegal activity. Its purpose is to determine the intensity of AML control: whether standard CDD is sufficient, whether enhanced due diligence is required, whether source-of-funds or source-of-wealth evidence must be obtained, whether senior management approval or MLRO review is needed, and whether refusal, termination or internal suspicious-activity assessment should be considered. The numerical score is a trigger for proportionate control and documented escalation, not a finding that money laundering has occurred.

The integration of the model into monitoring assisted by artificial intelligence (AI) should be subject to the principle that automation supports, but does not replace, expert judgment. In risk, audit and internal control practice, the most compelling organization is one in which primary signals from Transaction Monitoring Systems (TMS), Know Your Customer (KYC) files, Ultimate Beneficial Owner (UBO) data, sanctions checks, Politically Exposed Persons (PEP) checks and negative media coverage checks are translated into a specific task for the assessor. AI can draw attention to a change or non-compliance, but the decision to accept, limit or terminate a business relationship should remain a traceable expert decision.

At the input level, automation can extract and structure data from several sources: KYC file, ownership and representation registers, UBO declarations, contracts, invoices, payment accounts, historical transactions, sanction lists, PEP lists, results of checks for negative media publications and lists of high-risk jurisdictions. These data should not automatically determine the final risk. They serve as an evidentiary basis distributed across the three factors: entity and ownership data feed CE; payment characteristics and economic logic feed TI; and document quality, completeness, and verifiability feed CV.

At the assessment level, the model acts as an explainable layer between the automatically generated signal and the control measure. For example, an AI-assisted system or TMS built on predefined rules can report an unusual increase in the value of transactions, a new payment account, a change in jurisdiction, a negative media publication or a document leak. These signals do not automatically lead to a failure but activate a specific task: re-evaluation of the TI, re-verification of the CE, completion of the CV or a second internal review. Thus, the automatically generated signal is linked to a predefined control procedure and a documentary trail.

At the process level, the automated workflow can use clear grounds for updating the ORS: change in beneficial ownership or effective control; new intermediary; new high-risk jurisdiction; deviation of the value or frequency of operations from the expected profile; refusal or delay in providing key documents; contradiction between registry data and provided documents or a signal from a sanctions check, PEP check or negative media publication check. For each reason, the system can create a task, indicate the affected factor, request a specific document and register a deadline for completion.

The management limitation of automation is significant. At low and moderate risk, the system can support standard verification and periodic updating. At increased risk, it should require extended documentation and more frequent monitoring. At high and critical risk, automation should not replace human judgment but provide escalation to a competent person, Money Laundering Reporting Officer (MLRO), AML function or management. This preserves human participation in the decision-making process and reduces the risk of opaque or unfounded automatic decisions.

In this sense, the contribution to AI and automation is not a claim to self-prediction. The contribution is in explainability. The model transforms a multitude of qualitative and machine-generated signals into a limited number of verifiable factors, a formula, a classification threshold and a specific action. This makes it suitable for AML workflows, where regulatory defensibility requires not only signal detection, but also a demonstrable link between signal, assessment, decision and control measure.

The analysis of strengths, weaknesses, opportunities and threats (SWOT) systematizes the conditions for the correct application of the model (see Table 8). The strengths are related to the clear structure, the comparability of the results, the profile binding to specific control measures, the predefined classification thresholds and the possibility of automated updating. The limitations arise from the quality of the input information, possible differences between assessors, the need for future refinement and the risk that signals generated by AI will be perceived as evidence in themselves. The opportunities are related to implementation in internal procedures, TMS and AI-assisted systems, and the threats—to mechanical application without analysis, without updating, without expert review and without verification of the factual basis.

Table 8. SWOT matrix of the three-factor matrix model.

Strengths		Weaknesses	
✓	clear three-factor structure;	✓	dependence on the quality of input information;
✓	comparable result;	✓	possible differences between evaluators;
✓	relationship between risk level and control measures;	✓	need for future refinement of thresholds.
✓	good traceability of the assessment grounds.		
Opportunities		Threats	
✓	implementation in internal AML procedures;	✓	mechanical application without analysis;
✓	use in operations monitoring systems;	✓	failure to update as circumstances change;
✓	comparison between initial and updated risk;	✓	excessive reliance on numerical results without checking the factual basis.
✓	application in different sectors.		

Source: Prepared by the authors based on their own research.

A practical requirement follows from the SWOT matrix: each assessment must be documented, updated when significant changes occur and linked to a specific control action.

Despite the practical application on 25 profiles, the study retains important limitations. The array used has a purposively selected, application-oriented scope that is not statistically representative. Therefore, the results should not be interpreted as an estimate of the frequency of individual risk levels in a portfolio, sector or jurisdiction. Consistency between independent assessors was not measured, although the methodology introduces a documentary trail, a scoring rubric and a second review for higher-risk or borderline cases. These limitations define the appropriate use of the model as a structured assessment framework rather than as an externally validated predictive system.

Additional limitations should also be noted. The model has not been calibrated by sector, jurisdiction or institution type; it does not use full transaction time-series modelling; it does not assign empirically derived weights to the three factors; and it has not been tested against external AML outcomes such as STR/SAR decisions, regulatory findings or confirmed laundering cases. The 25 profiles are suitable for methodological demonstration because they contain AML-relevant variation, but they are not presented as the most representative or most severe cases in a wider portfolio. Future research should therefore test the model in banking, payment services, trade-related counterparties and digital-asset contexts, using larger datasets and independent expert panels.

6. Conclusions

This study developed and applied a three-factor matrix model for assessing counterparty risk in AML measures. The model combines counterparty exposure, transaction impact and control vulnerability, transforming qualitative information into an overall risk score and risk level. The application to 25 anonymized counterparty profiles demonstrates the procedural applicability of the model in assessment, documentation and selection of follow-up measures. The unordered presentation of the profiles, the profile-oriented control actions and the three-dimensional visualization enhance the transparency of the results, but they do not constitute external validation of predictive accuracy.

The main contribution is the inclusion of control vulnerability as an independent factor in the three-factor structure. Risk does not depend only on who the counterparty is and what operations it performs. It also depends on whether information about ownership, beneficial ownership, documents, operations and the origin of funds can be verified.

This logic is in line with the risk-based approach, customer due diligence and constant monitoring embedded in the modern European AML framework. In this way, the model links the scientific discussion of risk with a concrete assessment procedure.

The theoretical contribution is the translation of agency problems, information asymmetry and internal-control requirements into a concrete AML assessment sequence. The applied contribution is the creation of a documented link between FATF-style risk indicators, a factor score, a risk category and a proportionate AML control response.

The formula Overall Risk Score (ORS) = Counterparty Exposure (CE) × Transaction Impact (TI) × Control Vulnerability (CV) serves for classification and selection of subsequent actions. The product is used as a conservative and transparent aggregation rule for simultaneous accumulation across the three factors. The absence of preliminary weights is defensible in this initial model because weights should be empirically or expertly justified. The rating scale is managerial and is based on achievable values of the product; it should be interpreted together with the factor configuration and documentary basis of each assessment.

The practical value of the methodology is manifested in the relationship between the risk level and specific control measures. Low risk implies a standard comprehensive check and update in case of change. Moderate and increased risk require additional documents, analysis and more active monitoring. High and critical risk require enhanced due diligence, management decision, denial or termination when the risk cannot be reliably clarified. The model can also be used as explainable logic for AI-assisted TMS and AML monitoring, where automation detects changes and discrepancies, while human expert judgment remains the lead for high-risk decisions.

The limitations of the study are explicit. The practical application on 25 profiles has a purposively selected, application-oriented scope and does not allow generalization to an entire market, sector, jurisdiction or institution. Reliability between different raters has not been empirically verified. Future studies should apply the model to larger and more diverse samples, compare the multiplicative rule with additive, weighted, fuzzy-logic and AHP-based alternatives, test inter-rater agreement, calibrate thresholds against expert benchmarks or external AML outcomes where available, and examine implementation in automated monitoring systems under human oversight. Thus, the current model should be treated as a structured and explainable applied framework that can later be transformed into a more broadly tested risk management tool.

Author Contributions: Conceptualization, K.L. and N.V.-S.; methodology, K.L. and N.V.-S.; methodological application, K.L. and N.V.-S.; formal analysis, K.L. and N.V.-S.; investigation, K.L. and N.V.-S.; resources, K.L. and N.V.-S.; data curation and anonymization, K.L. and N.V.-S.; writing—original draft preparation, K.L. and N.V.-S.; writing—review and editing, K.L. and N.V.-S.; visualization, K.L. and N.V.-S.; supervision, K.L. and N.V.-S.; project administration, K.L.; funding acquisition, K.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the European Union—NextGenerationEU, through the National Recovery and Resilience Plan of the Republic of Bulgaria, grant number BG-RRP-2.004-0005. The APC was funded by the European Union—NextGenerationEU, through the National Recovery and Resilience Plan of the Republic of Bulgaria, grant number BG-RRP-2.004-0005.

Data Availability Statement: The data supporting the findings of this study are available from the corresponding author upon reasonable request. The underlying counterparty assessment profiles contain confidential business information and were anonymized for research purposes; therefore, the data are not publicly available.

Acknowledgments: This work has been accomplished with financial support by the European Regional Development Fund within the Operational Programme “Bulgarian national recovery and

resilience plan”, procedure for direct provision of grants “Establishment of a network of research higher education institutions in Bulgaria”, and under Project BG-RRP-2.004-0005 “Improving the research capacity and quality to achieve international recognition and resilience of TU-Sofia (IDEAS)”.

Conflicts of Interest: The authors declare no conflicts of interest. The funders had no role in the study design, data collection, analysis, or interpretation; in the writing of the manuscript; or in the decision to publish the results.

Abbreviations

The following abbreviations are used in this manuscript:

Abbreviation	Meaning
AHP	Analytic Hierarchy Process
AI	Artificial Intelligence
AML	Anti-Money Laundering
AMLA	Authority for Anti-Money Laundering and Countering the Financing of Terrorism
CDD	Customer Due Diligence
CE	Counterparty Exposure
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CV	Control Vulnerability
ERM	Enterprise Risk Management
FATF	Financial Action Task Force
KYC	Know Your Customer
MLRO	Money Laundering Reporting Officer
ORS	Overall Risk Score
PEP	Politically Exposed Persons
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report
SWOT	Strengths, Weaknesses, Opportunities and Threats
TI	Transaction Impact
TMS	Transaction Monitoring Systems
UBO	Ultimate Beneficial Owner

References

- Adaramola, Oluwabunmi. 2025. Assessing the role of the Intergovernmental Action Group Against Money Laundering in West Africa (GIABA) in light of virtual assets and cross-regional cryptocurrency-based money laundering in Nigeria. *Journal of Economic Criminology* 7: 100129. <https://doi.org/10.1016/j.jeconc.2025.100129>.
- Ai, Lishan. 2012. “Rule-based but risk-oriented” approach for combating money laundering in Chinese financial sectors. *Journal of Money Laundering Control* 15: 198–209. <https://doi.org/10.1108/13685201211218225>.
- Akerlof, George A. 1970. The market for “lemons”: Quality uncertainty and the market mechanism. *The Quarterly Journal of Economics* 84: 488–500. <https://doi.org/10.2307/1879431>.
- Aljassmi, Mariam, Awadh A. M. Gamal, Norasibah Abdul Jalil, and K. Kuperan Viswanathan. 2024. An analysis of the determinants of money laundering in the United Arab Emirates (UAE). *Journal of Money Laundering Control* 27: 858–72. <https://doi.org/10.1108/JMLC-09-2023-0150>.
- Allred, Brent B., Michael G. Findley, Daniel L. Nielson, and Jason C. Sharman. 2017. Anonymous shell companies: A global audit study and field experiment in 176 countries. *Journal of International Business Studies* 48: 596–619. <https://doi.org/10.1057/s41267-016-0047-7>.
- Andiojaya, Agung. 2025. Do stronger anti-money laundering (AML) measures reduce crime? An empirical study on corruption, bribery, and environmental crime. *Journal of Economic Criminology* 8: 100157. <https://doi.org/10.1016/j.jeconc.2025.100157>.
- Ardizzi, Guerino, Carmelo Petraglia, Massimiliano Piacenza, Friedrich Schneider, and Gilberto Turati. 2014. Money laundering as a crime in the financial sector: A new approach to quantitative assessment, with an application to Italy. *Journal of Money, Credit and Banking* 46: 1555–90. <https://doi.org/10.1111/jmcb.12159>.

- Aven, Terje. 2012. The risk concept—Historical and recent development trends. *Reliability Engineering & System Safety* 99: 33–44. <https://doi.org/10.1016/j.res.2011.11.006>.
- Aven, Terje. 2016. Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research* 253: 1–13. <https://doi.org/10.1016/j.ejor.2015.12.023>.
- Beebejaun, Ambareen. 2023. Compliance with anti-money laundering procedures by banks—The case of Mauritius. *Journal of Banking Regulation* 24: 474–83. <https://doi.org/10.1057/s41261-022-00211-6>.
- Bello, Abdullahi U., and Jackie Harvey. 2017. From a risk-based to an uncertainty-based approach to anti-money laundering compliance. *Security Journal* 30: 24–38. <https://doi.org/10.1057/s41284-016-0002-0>.
- Buchanan, Bonnie. 2004. Money laundering—A global obstacle. *Research in International Business and Finance* 18: 115–27. <https://doi.org/10.1016/j.ribaf.2004.02.001>.
- Chaikin, David A. 2009. How effective are suspicious transaction reporting systems? *Journal of Money Laundering Control* 12: 238–53. <https://doi.org/10.1108/13685200910973628>.
- Chen, Zhiyuan, Le Dinh Van Khoa, Ee Na Teoh, Amril Nazir, Ettikan Kandasamy Karuppiah, and Kim Sim Lam. 2018. Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: A review. *Knowledge and Information Systems* 57: 245–85. <https://doi.org/10.1007/s10115-017-1144-z>.
- Chitimira, Howard, and Sharon Munedzi. 2023. Overview international best practices on customer due diligence and related anti-money laundering measures. *Journal of Money Laundering Control* 26: 53–62. <https://doi.org/10.1108/JMLC-07-2022-0102>.
- Chong, Alberto, and Florencio Lopez-de-Silanes. 2015. Money laundering and its regulation. *Economics & Politics* 27: 78–123. <https://doi.org/10.1111/ecpo.12051>.
- Cohen, Jacob. 1960. A coefficient of agreement for nominal scales. *Educational and Psychological Measurement* 20: 37–46. <https://doi.org/10.1177/001316446002000104>.
- Committee of Sponsoring Organizations of the Treadway Commission (COSO). 1992. *Internal Control—Integrated Framework*. Jersey City: American Institute of Certified Public Accountants.
- Committee of Sponsoring Organizations of the Treadway Commission (COSO). 2004. *Enterprise Risk Management—Integrated Framework*. Jersey City: American Institute of Certified Public Accountants.
- Cox, Louis Anthony, Jr. 2008. What's wrong with risk matrices? *Risk Analysis* 28: 497–512. <https://doi.org/10.1111/j.1539-6924.2008.01030.x>.
- Dalla Pellegrina, Lucia, and Donato Masciandaro. 2009. The risk-based approach in the new European anti-money laundering legislation: A law and economics view. *Review of Law & Economics* 5: 931–52. <https://doi.org/10.2202/1555-5879.1422>.
- De Koker, Louis. 2009. Identifying and managing low money laundering risk: Perspectives on FATF's risk-based guidance. *Journal of Financial Crime* 16: 334–52. <https://doi.org/10.1108/13590790910993717>.
- Demetis, Dionysios S., and Ian O. Angell. 2007. The risk-based approach to AML: Representation, paradox, and the 3rd Directive. *Journal of Money Laundering Control* 10: 412–28. <https://doi.org/10.1108/13685200710830907>.
- Duijm, Nijs Jan. 2015. Recommendations on the use and design of risk matrices. *Safety Science* 76: 21–31. <https://doi.org/10.1016/j.ssci.2015.02.014>.
- Durguti, Esat, Erëza Arifi, Emine Gashi, and Muhamet Spahiu. 2023. Anti-money laundering regulations' effectiveness in ensuring banking sector stability: Evidence of Western Balkan. *Cogent Economics & Finance* 11: 2167356. <https://doi.org/10.1080/23322039.2023.2167356>.
- European Banking Authority. 2021. *Guidelines on Customer due Diligence and the Factors Credit and Financial Institutions Should Consider When Assessing the Money Laundering and Terrorist Financing Risk Associated with Individual Business Relationships and Occasional Transactions ('The ML/TF Risk Factors Guidelines') Under Articles 17 and 18(4) of Directive (EU) 2015/849*. EBA/GL/2021/02. Paris: European Banking Authority. Available online: https://www.eba.europa.eu/sites/default/files/document_library/Publications/Guidelines/2021/963637/Final%20Report%20on%20Guidelines%20on%20revised%20ML%20TF%20Risk%20Factors.pdf (accessed on 7 June 2026).
- European Parliament and Council of the European Union. 2024a. Directive (EU) 2024/1640 of 31 May 2024 on the Mechanisms to be Put in Place by Member States for the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing. *Official Journal of the European Union*, OJ L, 2024/1640, 19 June 2024. Available online: <https://eur-lex.europa.eu/eli/dir/2024/1640/oj/eng> (accessed on 2 June 2026).
- European Parliament and Council of the European Union. 2024b. Regulation (EU) 2024/1620 of 31 May 2024 Establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and Amending Regulations (EU) No 1093/2010,

- (EU) No 1094/2010 and (EU) No 1095/2010. *Official Journal of the European Union*, OJ L, 2024/1620, 19 June 2024. Available online: <https://eur-lex.europa.eu/eli/reg/2024/1620/oj/eng> (accessed on 4 June 2026).
- European Parliament and Council of the European Union. 2024c. Regulation (EU) 2024/1624 of 31 May 2024 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing. *Official Journal of the European Union*, OJ L, 2024/1624, 19 June 2024. Available online: <https://eur-lex.europa.eu/eli/reg/2024/1624/oj/eng> (accessed on 3 June 2026).
- EY. 2024. *Anti-Money Laundering (AML) Transaction Monitoring: 2024 Survey Report*. London: Ernst & Young LLP. Available online: <https://www.ey.com/content/dam/ey-unified-site/ey-com/en-uk/industries/financial-services/documents/ey-uk-aml-tm-survey-12-2024.pdf> (accessed on 8 June 2026).
- FATF. 2014. *Risk-Based Approach Guidance for the Banking Sector*. Paris: Financial Action Task Force. Available online: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Risk-based-approach-banking-sector.html> (accessed on 10 June 2026).
- FATF. 2019. *Guidance for a Risk-Based Approach for the Accounting Profession*. Paris: Financial Action Task Force. Available online: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Rba-accounting-profession.html> (accessed on 6 June 2026).
- FATF. 2021. *Opportunities and Challenges of New Technologies for AML/CFT*. Paris: Financial Action Task Force. Available online: <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf.coredownload.pdf> (accessed on 9 June 2026).
- FATF. 2025. *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations*. Paris: Financial Action Task Force. Available online: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html> (accessed on 2 June 2026).
- Favarel-Garrigues, Gilles, Thierry Godefroy, and Pierre Lascoumes. 2008. Sentinels in the banking industry: Private actors and the fight against money laundering in France. *British Journal of Criminology* 48: 1–19. <https://doi.org/10.1093/bjc/azm059>.
- Favarel-Garrigues, Gilles, Thierry Godefroy, and Pierre Lascoumes. 2011. Reluctant partners? Banks in the fight against money laundering and terrorism financing in France. *Security Dialogue* 42: 179–96. <https://doi.org/10.1177/0967010611399615>.
- Ferwerda, Joras. 2009. The economics of crime and money laundering: Does anti-money laundering policy reduce crime? *Review of Law & Economics* 5: 903–29. <https://doi.org/10.2202/1555-5879.1421>.
- Ferwerda, Joras, and Peter Reuter. 2024. National assessments of money laundering risks: Stumbling at the start. *Risk Analysis* 44: 2001–7. <https://doi.org/10.1111/risa.14302>.
- Fleiss, Joseph L. 1971. Measuring nominal scale agreement among many raters. *Psychological Bulletin* 76: 378–82. <https://doi.org/10.1037/h0031619>.
- Fronzetti Colladon, Andrea, and Eliana Remondi. 2017. Using social network analysis to prevent money laundering. *Expert Systems with Applications* 67: 49–58. <https://doi.org/10.1016/j.eswa.2016.09.029>.
- Geiger, Hans, and Oliver Wünsch. 2007. The fight against money laundering: An economic analysis of a cost-benefit paradoxon. *Journal of Money Laundering Control* 10: 91–105. <https://doi.org/10.1108/13685200710721881>.
- Gerbrands, Peter, Brigitte Unger, Michael Getzner, and Joras Ferwerda. 2022. The effect of anti-money laundering policies: An empirical network analysis. *EPJ Data Science* 11: 15. <https://doi.org/10.1140/epjds/s13688-022-00328-8>.
- Gilmour, Nicholas. 2016. Preventing money laundering: A test of situational crime prevention theory. *Journal of Money Laundering Control* 19: 376–96. <https://doi.org/10.1108/JMLC-10-2015-0045>.
- Haffke, Lars. 2023. Biases in risk assessments under EU anti-money laundering law—Evidence of the better-than-average effect from Germany. *Journal of Money Laundering Control* 26: 751–66. <https://doi.org/10.1108/JMLC-03-2022-0045>.
- Harvey, Jackie. 2008. Just how effective is money laundering legislation? *Security Journal* 21: 189–211. <https://doi.org/10.1057/palgrave.sj.8350054>.
- He, Ping. 2010. A typological study on money laundering. *Journal of Money Laundering Control* 13: 15–32. <https://doi.org/10.1108/13685201011010182>.
- Helgesson, Karin Svedberg, and Ulrika Mörrth. 2019. Instruments of securitization and resisting subjects: For-profit professionals in the finance–security nexus. *Security Dialogue* 50: 257–74. <https://doi.org/10.1177/0967010619835655>.
- Hubbard, Douglas W., and Dylan Evans. 2010. Problems with scoring methods and ordinal scales in risk assessment. *IBM Journal of Research and Development* 54: 2:1–2:10. <https://doi.org/10.1147/JRD.2010.2042914>.
- Jensen, Michael C., and William H. Meckling. 1976. Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics* 3: 305–60. [https://doi.org/10.1016/0304-405X\(76\)90026-X](https://doi.org/10.1016/0304-405X(76)90026-X).
- KPMG. 2025. *KPMG Blockchain Report 2024*. Zurich: KPMG AG. Available online: <https://assets.kpmg.com/content/dam/kpmg-sites/ch/pdf/kpmg-blockchain-report-2024.pdf.coredownload.pdf> (accessed on 6 June 2026).

- Kute, Dattatray V., Biswajeet Pradhan, Nagesh Shukla, and Abdullah M. Alamri. 2021. Deep learning and explainable artificial intelligence techniques applied for detecting money laundering—A critical review. *IEEE Access* 9: 82300–17. <https://doi.org/10.1109/ACCESS.2021.3086230>.
- Lagerwaard, Pieter. 2023. Financial surveillance and the role of the Financial Intelligence Unit (FIU) in The Netherlands. *Journal of Money Laundering Control* 26: 63–84. <https://doi.org/10.1108/JMLC-09-2022-0134>.
- Lagerwaard, Pieter, and Marieke de Goede. 2023. In trust we share: The politics of financial intelligence sharing. *Economy and Society* 52: 202–26. <https://doi.org/10.1080/03085147.2023.2175451>.
- Landis, J. Richard, and Gary G. Koch. 1977. The measurement of observer agreement for categorical data. *Biometrics* 33: 159–74. <https://doi.org/10.2307/2529310>.
- Levi, Michael. 2002. Money laundering and its regulation. *The Annals of the American Academy of Political and Social Science* 582: 181–94. <https://doi.org/10.1177/000271620258200113>.
- Levi, Michael. 2015. Money for crime and money from crime: Financing crime and laundering crime proceeds. *European Journal on Criminal Policy and Research* 21: 275–97. <https://doi.org/10.1007/s10610-015-9269-7>.
- Levi, Michael. 2020. Evaluating the control of money laundering and its underlying offences: The search for meaningful data. *Asian Journal of Criminology* 15: 301–20. <https://doi.org/10.1007/s11417-020-09319-y>.
- Levi, Michael, and Peter Reuter. 2006. Money laundering. *Crime and Justice* 34: 289–375. <https://doi.org/10.1086/501508>.
- Lokanan, Mark Eshwar, and Noor Nasimi. 2020. The effectiveness of anti-money laundering policies and procedures within the banking sector in Bahrain. *Journal of Money Laundering Control* 23: 769–81. <https://doi.org/10.1108/JMLC-10-2019-0080>.
- Masciandaro, Donato. 1999. Money laundering: The economics of regulation. *European Journal of Law and Economics* 7: 225–40. <https://doi.org/10.1023/A:1008776629651>.
- Meiryani. 2024. Prevention and control of money laundering crimes on know your customer principles application: Empirical study of Indonesia banking sector. *Journal of Money Laundering Control* 27: 873–85. <https://doi.org/10.1108/JMLC-01-2023-0008>.
- Nazar, Sadia, Abdul Raheman, and Muhammad Anwar ul Haq. 2024. The magnitude and consequences of money laundering. *Journal of Money Laundering Control* 27: 808–24. <https://doi.org/10.1108/JMLC-09-2022-0139>.
- Ofoeda, Isaac. 2022. Anti-money laundering regulations and financial inclusion: Empirical evidence across the globe. *Journal of Financial Regulation and Compliance* 30: 646–64. <https://doi.org/10.1108/JFRC-12-2021-0106>.
- Ogbeide, Henry, Mary E. Thomson, Mustafa S. Gönül, Andrew C. Pollock, Sanjay Bhowmick, and Abdullahi U. Bello. 2023. The anti-money laundering risk assessment: A probabilistic approach. *Journal of Business Research* 162: 113820. <https://doi.org/10.1016/j.jbusres.2023.113820>.
- Ogbeide, Henry, Mary E. Thomson, Mustafa S. Gönül, Dilek Önköl, Sanjay Bhowmick, and Abdullahi U. Bello. 2025. Rethinking experts' perceptions in money laundering risk assessment. *European Journal on Criminal Policy and Research* 31: 753–77. <https://doi.org/10.1007/s10610-024-09586-w>.
- Peace, Christopher. 2017. The risk matrix: Uncertain results? *Policy and Practice in Health and Safety* 15: 131–44. <https://doi.org/10.1080/14773996.2017.1348571>.
- Pol, Ronald F. 2018. Anti-money laundering effectiveness: Assessing outcomes or ticking boxes? *Journal of Money Laundering Control* 21: 215–30. <https://doi.org/10.1108/JMLC-07-2017-0029>.
- Pol, Ronald F. 2020. Anti-money laundering: The world's least effective policy experiment? Together, we can fix it. *Policy Design and Practice* 3: 73–94. <https://doi.org/10.1080/25741292.2020.1725366>.
- PwC. 2024. *EMEA AML Survey 2024: UK Insights on Effectiveness*. London: PricewaterhouseCoopers. Available online: <https://www.pwc.co.uk/financial-services/assets/pdf/emea-aml-survey-2024.html.pdf> (accessed on 10 June 2026).
- Riccardi, Michele. 2025. A data-driven approach to measure money laundering risk and its relationship with corruption. *Journal of Economic Criminology* 10: 100184. <https://doi.org/10.1016/j.jeconc.2025.100184>.
- Saaty, Thomas L. 2008. Decision making with the analytic hierarchy process. *International Journal of Services Sciences* 1: 83–98. <https://doi.org/10.1504/IJSSCI.2008.017590>.
- Schneider, Friedrich, and Ursula Windischbauer. 2008. Money laundering: Some facts. *European Journal of Law and Economics* 26: 387–404. <https://doi.org/10.1007/s10657-008-9070-x>.
- Sharman, Jason C. 2010. Shopping for anonymous shell companies: An audit study of anonymity and crime in the international financial system. *Journal of Economic Perspectives* 24: 127–40. <https://doi.org/10.1257/jep.24.4.127>.
- Simonova, Anna. 2011. The risk-based approach to anti-money laundering: Problems and solutions. *Journal of Money Laundering Control* 14: 346–58. <https://doi.org/10.1108/13685201111173820>.

- Singh, Kishore, and Peter Best. 2019. Anti-money laundering: Using data visualization to identify suspicious activity. *International Journal of Accounting Information Systems* 34: 100418. <https://doi.org/10.1016/j.accinf.2019.06.001>.
- Takáts, Előd. 2011. A theory of “crying wolf”: The economics of money laundering enforcement. *Journal of Law, Economics, and Organization* 27: 32–78. <https://doi.org/10.1093/jleo/ewp018>.
- Teichmann, Fabian M. J. 2017. Twelve methods of money laundering. *Journal of Money Laundering Control* 20: 130–37. <https://doi.org/10.1108/JMLC-05-2016-0018>.
- Tiwari, Milind, Adrian Gepp, and Kuldeep Kumar. 2020. A review of money laundering literature: The state of research in key areas. *Pacific Accounting Review* 32: 271–303. <https://doi.org/10.1108/PAR-06-2019-0065>.
- Unger, Brigitte, and Greg Rawlings. 2008. Competing for criminal money. *Global Business and Economics Review* 10: 331–52. <https://doi.org/10.1504/GBER.2008.019987>.
- Walker, John, and Brigitte Unger. 2009. Measuring global money laundering: The Walker Gravity Model. *Review of Law & Economics* 5: 821–53. <https://doi.org/10.2202/1555-5879.1418>.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.