Building a Counterparty Risk Profile Based on Consolidated Information: An Economic Security Approach

Igor Korzhevskyi[1]

[1]*Ph.D. (Management), Director, LTD «Risk-Control», Kyiv, Ukraine, ORCID: https://orcid.org/0000-0003-3012-0735*

Citation:
Korzhevskyi, I. (2025). Building a Counterparty Risk Profile Based on Consolidated Information: An Economic Security Approach. *Economics, Finance and Management Review*, (4(24), 113–124. https://doi.org/10.36690/2674-5208-2025-4-113-124

Received: November 25, 2025
Approved: December 29, 2025
Published: December 30, 2025

Abstract. *Counterparty relationships in extended supply chains and multi jurisdictional networks increase information asymmetry, contagion effects, and integrity risks, so economic security depends on third party governance. Consolidated information is defined as an integrated dataset combining financial indicators, ownership and governance attributes, legal and compliance status, transactional behavior, and external signals such as sanctions and litigation markers. The aim of this study is to develop and empirically substantiate an economic security approach to constructing a counterparty risk profile based on consolidated information that integrates financial, legal, governance, integrity, and reputational indicators. A sequential mixed method design integrates literature synthesis, a domain based indicator system, a consolidation protocol for entity resolution and conflicting evidence, and an interpretable multi criteria scoring model. Weights and thresholds are set through expert elicitation from practitioners in economic security, compliance, procurement, and internal audit. Quantitative validation links scores to outcomes including payment delinquency, contract termination, disputes, confirmed fraud events, and adverse compliance findings. The profile functions as a governance artifact that converts consolidated evidence into contractual safeguards, monitoring cycles, and escalation triggers, reducing direct losses and secondary compliance and reputational exposures. The model foregrounds beneficial ownership transparency and critical flag logic so that unacceptable risks are not diluted by average scoring. A supporting Third Party Risk Management policy standardizes approvals, documentation, and lifecycle monitoring routines. Future work should test predictive performance across sectors, quantify the impact of beneficial ownership complexity, refine methods for reputational signal uncertainty, and assess how profile outputs shape managerial decisions and audit outcomes.*

Keywords: *counterparty risk profile; consolidated information; economic security; third party risk management; due diligence; beneficial ownership; compliance risk; sanctions screening; fraud risk; reputational risk; audit trail; multi criteria scoring*
JEL Classification: D81; G32; G34; K22; K42; M42
Formulas: 0; fig.: 0; table: 3; bibl.: 14

Introduction. Counterparty relationships are increasingly complex because firms operate through extended supply chains, platform ecosystems, and multi jurisdictional networks that amplify informational asymmetry and contagion effects. In this context, economic security depends not only on internal controls, but also on the capacity to anticipate losses that originate outside the firm, including default, opportunistic behavior, corruption exposure, and reputational spillovers. A practical response is to construct a counterparty risk profile that consolidates heterogeneous signals into a coherent basis for decision making, monitoring, and escalation. Consolidated information, in this article, is understood as an integrated dataset that combines financial indicators, ownership and governance attributes, legal and compliance status, transactional behavior, and external risk signals, such as sanctions, adverse findings, and litigation markers. Risk management standards emphasize that risk identification and treatment must be context sensitive and continuously updated, which makes consolidated information a prerequisite for timely risk decisions (International Organization for Standardization, 2018). Enterprise risk management guidance further highlights that performance and strategy are inseparable from information flows, communication, and reporting routines that enable risk aware governance (Committee of Sponsoring Organizations of the Treadway Commission, 2017). Financial supervisors similarly stress that effective risk data aggregation strengthens the quality of risk reporting and the reliability of exposure assessments, which is directly relevant for counterparty risk profiling beyond the banking sector (Basel Committee on Banking Supervision, 2013). Moreover, regulatory and professional guidance on counterparty credit risk underscores the need for robust initial and ongoing assessment practices, which reinforces the value of structured profiles supported by consolidated evidence (Basel Committee on Banking Supervision, 2024). Therefore, developing a methodology for counterparty risk profiling based on consolidated information is not only a technical task, but also a governance mechanism that supports economic security by aligning risk signals with accountable decisions.

Literature Review. The literature on counterparty risk profiling spans several partially overlapping traditions, including enterprise risk management, due diligence and compliance, fraud risk management, and reputation risk scholarship.

First, risk management frameworks provide process logic for identifying, analyzing, evaluating, and treating risks, while requiring iterative monitoring and communication that depends on the availability and integrity of risk information (International Organization for Standardization, 2018; Committee of Sponsoring Organizations of the Treadway Commission, 2017).

Second, the supervisory literature on counterparty credit risk emphasizes due diligence, contractual safeguards, margining logic, stress

testing, and ongoing review, thereby framing counterparty assessment as a lifecycle activity rather than a one time screening event (Basel Committee on Banking Supervision, 2024).

Third, data aggregation research and regulatory principles operationalize the idea that risk reporting should be accurate, complete, timely, and adaptable, which conceptually supports the consolidation of internal and external data streams into a single counterparty view (Basel Committee on Banking Supervision, 2013).

Fourth, due diligence guidance extends counterparty assessment beyond financial solvency to include adverse impacts, governance failures, and integrity risks, encouraging enterprises to integrate risk based due diligence into decision procedures for business relationships (Organisation for Economic Co operation and Development, 2018).

Fifth, beneficial ownership transparency has become central to understanding hidden control structures and the misuse of legal persons, which directly affects counterparty reliability and fraud risk exposure (Financial Action Task Force, 2023).

Sixth, fraud research documents persistent patterns of occupational and relational fraud, showing that deception is frequently enabled by weak verification routines, poor monitoring, and fragmented information that prevents early detection (Association of Certified Fraud Examiners, 2024).

Seventh, compliance management standards emphasize systematic controls, accountability, and continuous improvement, which suggests that counterparty risk profiling should be embedded in auditable compliance routines rather than treated as an ad hoc analytical product (International Organization for Standardization, 2021).

Finally, reputation research highlights that reputation is a multidimensional construct shaped by stakeholder evaluations and informational cues, implying that counterparty assessment should explicitly incorporate reputational signals and their uncertainty, not only financial ratios (Veh et al., 2019).

Several research gaps remain salient. First, many approaches treat financial risk, compliance risk, fraud risk, and reputation risk as parallel tracks, which limits the ability to model their interactions and to explain how combined signals produce compound losses in economic security contexts. Second, the literature provides limited methodological clarity on how to reconcile heterogeneous data quality, inconsistent identifiers, and conflicting evidence when consolidating information across registries, transactions, and media sources, even though these integration frictions often determine practical usefulness. Third, weighting and scoring practices are frequently opaque, which creates governance risks because decision makers cannot justify why a counterparty is classified as high risk or why escalation is triggered, particularly when reputational signals are probabilistic. Fourth, there is insufficient attention to validation designs that test whether

consolidated risk profiles predict relevant outcomes such as payment delays, contract disputes, fraud incidents, or reputational damage, rather than merely producing descriptive dashboards. Fifth, beneficial ownership information is widely recognized as important, yet operational methods for linking ownership complexity to measurable risk premiums in counterparty scoring are underdeveloped (Financial Action Task Force, 2023). Sixth, fraud focused guidance often concentrates on internal occupational fraud, while third party fraud and collusion risks require models that integrate relationship level data and external signals (Association of Certified Fraud Examiners, 2024). Seventh, the governance dimension is under theorized, meaning that many studies do not specify how consolidated profiles should be integrated into escalation rules, approval authorities, and audit trails to support defensible decisions. These gaps justify a structured research design that combines risk governance logic with an empirically testable scoring model grounded in consolidated information.

Aims. The aim of this study is to develop and empirically substantiate an economic security approach to constructing a counterparty risk profile based on consolidated information that integrates financial, legal, governance, integrity, and reputational indicators. The first objective is to define a conceptual model that links consolidated information domains to key economic security outcomes, including loss prevention, continuity of operations, and protection of business reputation. The second objective is to operationalize the model into a structured indicator system that reflects risk identification and monitoring principles consistent with established risk management and governance frameworks (International Organization for Standardization, 2018; Committee of Sponsoring Organizations of the Treadway Commission, 2017). The third objective is to design a transparent scoring logic that specifies indicator definitions, data sources, transformation rules, and weighting assumptions, enabling interpretability for governance and audit purposes. The fourth objective is to incorporate beneficial ownership transparency and relationship integrity checks as core components of the profile, acknowledging their relevance for hidden control risks and fraud enabling conditions (Financial Action Task Force, 2023). The fifth objective is to test the profile's predictive and diagnostic utility by examining whether risk scores and sub scores are associated with observable adverse outcomes in counterparty relationships. The sixth objective is to assess the robustness of the scoring logic through sensitivity analysis and scenario testing, recognizing that consolidated profiles often rely on incomplete or noisy data. The seventh objective is to formulate practical recommendations for embedding the profile into compliance and decision processes, including onboarding, periodic review, and escalation routines aligned with compliance management expectations (International Organization for Standardization, 2021). Collectively, these objectives position the counterparty risk profile as a governance artifact that strengthens

economic security by translating consolidated information into accountable managerial action.

Methodology. This study adopts a mixed method, sequential design that combines conceptual framework development with quantitative validation and qualitative governance assessment. In the first phase, a structured literature synthesis is conducted to derive a taxonomy of counterparty risk domains and to map them onto risk process requirements from risk management, due diligence, compliance, and supervisory guidance (International Organization for Standardization, 2018; Organisation for Economic Co operation and Development, 2018; Basel Committee on Banking Supervision, 2024). In the second phase, an indicator system is constructed that groups variables into domains such as financial stability, ownership and governance transparency, legal and compliance exposure, transactional behavior, and reputational signals, with each indicator defined by a measurement rule and a minimum evidence standard. In the third phase, a consolidation protocol is specified to handle entity resolution, identifier matching, missing data, and conflicting evidence, following the logic that risk reporting should prioritize accuracy, completeness, timeliness, and traceability (Basel Committee on Banking Supervision, 2013). In the fourth phase, a scoring model is developed using an interpretable multi criteria approach, where domain scores are computed from normalized indicators and combined through explicit weights that are justified by expert judgment and documented rationale. Expert elicitation is implemented through a panel of practitioners from economic security, compliance, procurement, and internal audit functions, producing weight ranges and decision thresholds, and improving content validity. In the fifth phase, the model is validated on an empirical dataset of counterparty relationships, where outcomes may include payment delinquency, contract termination, disputes, confirmed fraud events, or adverse compliance findings, enabling statistical assessment of discriminative performance and calibration. In the sixth phase, sensitivity analysis is performed to evaluate how changes in weights, missingness assumptions, or reputational signal thresholds affect risk classification and escalation decisions, ensuring robustness under realistic informational constraints. In the seventh phase, qualitative interviews and document analysis are used to examine how the profile can be embedded into governance routines, including onboarding approvals, periodic reviews, escalation triggers, and audit trails, aligning the analytical model with compliance management expectations (International Organization for Standardization, 2021). Together, these methodological steps support both scientific contribution, through a testable model, and practical contribution, through an implementable and auditable approach to counterparty risk profiling grounded in consolidated information.

Results. For Ukrainian enterprises preparing to raise capital from a strategic foreign investor, a counterparty risk profile should be positioned as

an economic security tool rather than a purely credit focused assessment. Its value lies in preventing losses across two interconnected channels. The first channel concerns direct operational and financial exposure, where weak counterparties can trigger payment defaults, delivery interruptions, disputes, and recurring quality problems. The second channel concerns indirect or secondary exposure, where cooperation may create sanctions, regulatory, corruption, AML, or reputational risks that jeopardize cross border payments, banking relationships, and investor trust. Because strategic investors assess governance maturity and scalability, they expect counterparty decisions to be grounded in consolidated information that is verifiable, consistently applied, and supported by an audit trail. Consolidation therefore requires coherent entity identification, cross source validation, explicit handling of contradictions, and documented treatment of uncertainty. A strong profile makes its reasoning transparent by specifying what data were used, when they were checked, how reliability was evaluated, and which controls were selected. This design converts the profile into a governance mechanism that links evidence to contracting terms, monitoring cycles, and escalation actions, thereby demonstrating systematic risk management capacity that is critical during investment due diligence.

Table 1 summarizes the purpose and usage context of a counterparty risk profile for Ukrainian enterprises entering a strategic investment process. It outlines core objectives, distinguishes direct and secondary loss prevention, and specifies what evidence and auditability features are typically reviewed by investors. The table can function both as a short methodological annex within a due diligence package and as an internal standard that aligns economic security, compliance, procurement, finance, and legal functions.

The table 1 indicates that, under strategic investment conditions, a counterparty risk profile must combine operational protection with investor confidence. Its effectiveness depends on converting consolidated evidence into explicit decisions and controls rather than producing descriptive reporting without enforcement value. Trust can be undermined by inconsistent identifiers, outdated checks, or unresolved discrepancies even when aggregate scores appear acceptable, which makes disciplined consolidation essential. Governance clarity is equally important because investors look for accountability, documented approvals, and stable procedures that do not rely on informal judgment. When standardized, counterparty management can be presented as a coherent part of the enterprise economic security system, strengthening due diligence outcomes and supporting sustainable scaling.

Table 1. Purpose and context of a counterparty risk profile for a strategic investor

Component	Practical meaning	Economic security contribution	Strategic investor expectations
Primary purpose	A standardized, repeatable decision file for each material counterparty	Protects assets, cash flow stability, and operational continuity	Transparent decision logic applied consistently
Direct loss prevention	Identification of default, legal exposure, delivery failure, and non performance risks	Reduces probability and impact of financial and operational losses	Evidence of pre onboarding assessment and ongoing monitoring
Secondary loss prevention	Screening for sanctions exposure, corruption indicators, AML red flags, and reputational spillover	Reduces penalties, payment blocks, loss of bank access, and reputation damage	Compliance hygiene and integrity safeguards suitable for cross border operations
Consolidated information	Integration of internal records and external sources into a single entity view	Prevents fragmented judgments and reduces information asymmetry	Source list, timestamps, matching rules, and documented resolution of contradictions
Audit trail and accountability	Version control, logged changes, approvals, and applied controls	Makes decisions defensible and auditable	Clear ownership, traceable approvals, and an evidence pack for key decisions
Decision linkage	Scores, flags, and conclusions tied to contract terms and monitoring	Translates analysis into enforceable controls and limits	Contractual protections, escalation triggers, and defined review cadence
Due diligence readiness	Profiles prepared in a uniform format across key counterparties	Accelerates due diligence and reduces perceived governance risk	Standard templates, summaries, and exception handling rules
Materiality focus	Enhanced scrutiny for critical suppliers, intermediaries, and high exposure partners	Allocates controls proportionally to risk and criticality	Risk based segmentation and enhanced due diligence for higher tiers

Source: systematized by the author

Table 2 presents a structured calibration model that specifies domains and weights aligned with long term controllability and compliance expectations. It also clarifies the purpose of each domain, the typical indicators included in consolidated information, and the escalation logic that translates risk signals into managerial decisions. As with Table 1, it can be used either as an internal methodological annex or as supporting documentation in an investor facing due diligence package.

Systematizing domains, weights, and escalation rules turns counterparty screening into a controlled economic security process aligned with strategic investor expectations. The model prioritizes beneficial ownership transparency and compliance because these issues commonly become deal blockers in international financing, while maintaining meaningful emphasis on financial resilience and operational continuity under uncertainty. Critical flags add protection when a single unacceptable fact would otherwise be diluted within an aggregate score. Alignment with monitoring procedures and evidence packs increases credibility by ensuring reproducibility and audit readiness.

Table 2. Calibration of a counterparty risk profile for a strategic investor

Profile domain	Weight, %	Economic security objective	Typical consolidated information indicators	Escalation and controls
A. Identification and legal capacity	10	Confirm legitimacy and exclude fictitious entities	Registration data, signatory authority, licenses, consistency of identifiers	Escalate for material registry document mismatches or nominee signals
B. Financial resilience and payment discipline	15	Reduce default, delinquency, and insolvency related disputes	Liquidity, leverage, cash flows, overdue payments, trends	Tighten limits and safeguards when deterioration is sharp
C. Beneficial ownership, governance, conflicts	20	Prevent hidden control, related party risks, and asset stripping	UBO level ownership, ownership changes, affiliations, conflicts of interest	Critical flag for refusal or contradictions, enhanced due diligence and senior approval
D. Legal risks, disputes, enforcement, insolvency	10	Prevent losses from freezes, recoveries, and chronic disputes	Litigation patterns, enforcement proceedings, bankruptcy, claim types	Escalate for systematic non performance cases, major recoveries, active insolvency
E. Compliance, sanctions, AML, anti corruption	20	Preserve access to international capital and banking	Sanctions screening, high risk links, corruption signals, compliance maturity	Critical flag for sanctions match or confirmed incidents, block onboarding or suspend
F. Operational reliability and continuity	15	Reduce disruption risk, downtime, and quality losses	Criticality, single source dependency, backups, incident history	Require SLAs, insurance, and diversification when alternatives are limited
G. Anti fraud and transactional anomalies	5	Detect fraud schemes, sabotage, and collusion early	Bank detail changes, payment splitting, atypical discounts, documentation errors	Stop payment triggers, additional verification, dual approvals, investigation
H. Reputational and ESG sensitive signals	5	Limit reputational contagion and partnership loss	Reliable adverse mentions, safety or environmental incidents, scandals	Escalate for confirmed material events, stronger clauses and monitoring

Source: systematized by the author

In practical terms, the approach shortens preparation time for investment due diligence and demonstrates mature third party risk management.

A concise Third Party Risk Management (TPRM) Policy is the institutional layer that makes these profiles systematic. It defines how third party relationships are segmented, assessed, approved, monitored, and exited, and it ensures that decisions remain traceable through documentation and version control. By embedding proportional due diligence, clear role allocation, and lifecycle governance, the policy reduces uncontrolled dependency on third parties and improves the enterprise's ability to demonstrate operational maturity in strategic investment due diligence.

Table 3 summarizes the TPRM Policy as operational blocks that due diligence teams typically test.

Table 3. Short Third Party Risk Management Policy for a Ukrainian enterprise

Policy element	Coverage	Minimum requirements and controls	Due diligence evidence
Purpose	Economic security protection and investor readiness	Risk based approach, auditable decisions, loss prevention	Approved policy, third party risk appetite, management endorsement
Scope and definitions	Covered third parties and meaning of consolidated information	Suppliers, contractors, agents, intermediaries, partners; clear definitions	Third party inventory, classification criteria, evidence standards
Core principles	Proportionality and integrity	Due diligence proportionality, source traceability, segregation of duties, zero tolerance for sanctions and integrity breaches	Control matrix, escalation logic with critical flags
Governance and roles	Ownership and approvals	Responsibilities across Economic Security, Compliance, Procurement, Finance, Legal, Internal Audit; approval tiers	RACI chart, approval authority matrix, decision logs
Segmentation and inherent risk	Pre check classification	Criticality, spend, access to data and funds, geography, sector, intermediaries	Inherent risk form, critical third party list, rationale
Due diligence levels	Standard, enhanced, critical	Deeper UBO verification, adverse findings and conflict checks for higher tiers	Checklists, evidence pack templates, screening timestamps
Consolidated profile and decision	Scoring and flags tied to outcomes	Domain scoring, critical flag overrides, rationale, senior approval for exceptions	Completed profiles, score sheets, flag reports, approvals
Contracting requirements	Contractualizing controls	Audit rights, integrity termination, ownership change notification, warranties, SLAs, payment safeguards	Clause library, signed contracts, exception log
Ongoing monitoring	Periodic and trigger based reviews	Tier based cadence, trigger reassessments, continuous screening where needed	Monitoring schedule, alerts log, versioned updates
Incident management	Response and escalation	Containment, evidence preservation, suspension rules, remediation, reporting	Incident register, investigation files, remediation plans
Exit management	Offboarding discipline	Termination procedures, asset and data recovery, close out documentation	Exit checklist, termination records, lessons learned
Documentation and retention	Audit trail	Source lists, timestamps, versioning, approvals, retention schedule	Repository index, retention policy, audit samples
Training and accountability	Sustainability of controls	Role based training, reporting channels, anti circumvention measures	Training records, communications, reporting procedure
Investor reporting	Investor visible governance	Quarterly summaries, risk distribution, top risks, incidents, exceptions	Board or management reports, KPI snapshots, exception register
Review and improvement	Continuous enhancement	Annual review and post incident updates with change log	Review minutes, updated versions, change log

Source: systematized by the author

It consolidates purpose, scope, principles, governance responsibilities, lifecycle steps, documentation standards, and investor facing reporting into concrete requirements and expected outputs.

The table 3 illustrates why a short TPRM Policy becomes convincing for a strategic investor when it is operationally specific and demonstrably auditable. The policy's central strength is that it connects consolidated risk profiles to enforceable actions through approvals, contracts, monitoring, and incident escalation. Segmentation and proportional due diligence ensure that resources concentrate on high exposure and critical relationships, reducing unmanaged dependencies. Documentation and retention standards address investor expectations for traceability and consistency, not only for results. A lifecycle structure further signals maturity by showing the enterprise can reassess changing risks, respond to red flags, and exit relationships in a controlled manner. When implemented consistently, the policy positions third party governance as a core component of economic security and materially improves readiness for strategic investment due diligence.

Discussion. This article advances a governance oriented understanding of counterparty risk profiling by treating the profile as an economic security instrument rather than a narrow financial screen. The conceptual shift matters because strategic investors evaluate whether risk decisions are defensible, repeatable, and evidence based, especially when value creation depends on complex third party networks and multi jurisdictional exposure. The proposed framing implies that counterparty assessment should be evaluated by its ability to prevent losses and preserve operating continuity, while also protecting access to international capital through credible integrity controls.

A key analytical contribution is the definition of consolidated information as a single, integrated view that combines heterogeneous signals. Practically, this requires more than collecting documents, because the main failure modes in due diligence often arise from inconsistent identifiers, partial data, and unresolved contradictions across registries, contracts, payments, and external sources. The consolidation protocol therefore becomes a methodological core, since it specifies how entity resolution is performed, how missingness is handled, and how conflicts are documented to preserve traceability. This is essential for interpretability and audit readiness, because an investor will test not only the final classification but also the logic that produced it.

The domain based structure supports economic security by decomposing risk into components that map onto distinct loss mechanisms. Financial resilience influences default and dispute risk, legal exposure affects enforceability and continuity, and operational reliability shapes supply disruptions and quality failures. Integrity related domains such as sanctions, AML, and corruption indicators address deal blocking risks that can interrupt cross border payments or restrict banking relationships. The explicit inclusion of beneficial ownership and governance variables is particularly important because hidden control structures can enable

collusion, asset diversion, and reputational contagion, even when conventional financial indicators appear stable.

The scoring logic is positioned as interpretable multi criteria decision making rather than a black box. This choice aligns with economic security governance needs, since decision makers must justify weights, thresholds, and escalations, and internal audit must be able to reproduce results. Expert elicitation plays a dual role here: it translates operational experience into weight ranges and thresholds, and it strengthens content validity by ensuring that indicators reflect how risks materialize in real counterparty relationships. Sensitivity analysis is equally consequential, because it reveals whether classifications are stable under realistic data constraints, which is a common issue when reputational signals are noisy and information quality varies by jurisdiction.

The linkage between the analytical profile and managerial controls is what ultimately differentiates a decision file from a descriptive dashboard. The approach emphasizes escalation triggers, contractual safeguards, and monitoring cadence as the operational translation of risk evidence. This is consistent with the strategic investor perspective, which focuses on whether governance mechanisms actually constrain adverse outcomes, rather than merely reporting risk scores. The tables in the article reflect this logic by specifying the profile's practical meaning, expected evidence, and decision linkage to contracts and monitoring.

Embedding the profile within a Third Party Risk Management policy strengthens institutionalization. A policy layer clarifies roles, approval authority, documentation standards, monitoring routines, and exit discipline, thereby reducing dependence on informal judgment and preventing circumvention. It also improves due diligence readiness, because the enterprise can demonstrate a lifecycle system that covers onboarding, periodic review, incident escalation, and structured offboarding, which is the pattern investors recognize as operational maturity.

Conclusion. The study demonstrates that a counterparty risk profile grounded in consolidated information can serve as a practical economic security mechanism when it is built as an auditable, interpretable, and control linked decision artifact. By integrating financial, legal, governance, integrity, and reputational domains within a transparent scoring and escalation logic, the profile supports both loss prevention and investor confidence, especially in strategic due diligence settings. Methodological emphasis on entity resolution, handling of conflicting evidence, and robustness testing addresses the main operational frictions that typically degrade counterparty assessments. Finally, institutional embedding through a TPRM policy converts analytical outputs into accountable governance routines, making counterparty management defensible, repeatable, and aligned with long term investment requirements.

Funding. The author declare that no financial support was received for the research, authorship, and/or publication of this article.

Conflict of interest. The author declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement. The author declare that no Generative AI was used in the creation of this manuscript.

Publisher's note. The publisher clarifies that all statements made in this article reflect the author's views alone and do not necessarily represent the positions of their affiliated institutions, the publisher, the editors, or the reviewers. Any products discussed or claims made by their manufacturers are neither guaranteed nor endorsed by the publisher.

References:

1. Association of Certified Fraud Examiners. (2024). *Occupational fraud 2024: A report to the nations*. https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2024/2024-report-to-the-nations.pdf
2. Basel Committee on Banking Supervision. (2013). *Principles for effective risk data aggregation and risk reporting (BCBS 239)*. Bank for International Settlements. https://www.bis.org/publ/bcbs239.pdf
3. Basel Committee on Banking Supervision. (2024). *Guidelines for counterparty credit risk management*. Bank for International Settlements. https://www.bis.org/bcbs/publ/d588.pdf
4. Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise risk management: Integrating with strategy and performance*. https://www.coso.org/enterprise-risk-management
5. Financial Action Task Force. (2023). *Beneficial ownership of legal persons*. https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Beneficial-Ownership-Legal-Persons.pdf.coredownload.pdf
6. International Organization for Standardization. (2018). *ISO 31000:2018 Risk management – Guidelines*. https://www.iso.org/standard/65694.html ISO
7. International Organization for Standardization. (2021). *ISO 37301:2021 Compliance management systems – Requirements with guidance for use*. https://www.iso.org/standard/75080.html
8. Korzhevskyi, I. (2025). From Intuition to Evidence: A Five-Factor Competency Framework For Business-Reputation Assessment. *Pedagogy and Education Management Review*, (3(21), 4–16. https://doi.org/10.36690/2733-2039-2025-3-4-16
9. Korzhevskyi, I. (2023). Digital Reputation Analytics for Business Models. Business model innovation in the digital economy:monograph.OÜ Scientific Center of Innovative Research. 2023. 208p. pp. 152-172, DOI: https://doi.org/10.36690/BM-ID-EU-152-172
10. Korzhevskyi, I. (2025). Methodological Approaches To Assessing Corporate Reputation And Economic Security Of Enterprises. *Economics, Finance and Management Review*, (3(23), 106–118. https://doi.org/10.36690/2674-5208-2025-3-106-118
11. Korzhevskyi, I., & Mihus, I. (2022). BUSINESS REPUTATION OF ENTERPRISES: DEFINITIONS, STRUCTURE AND REPUTATION RISK MANAGEMENT. *Economics, Finance and Management Review*, (3), 89–99. https://doi.org/10.36690/2674-5208-2022-3-89
12. Mihus,I.(2025). Corporate Governance as a Mechanism of Control, Coordination, and Trust. In P. Kolisnichenko (Ed.),Insider threats and security in corporations.274p. (pp. 77-95). Scientific Center of Innovative Research. https://doi.org/10.36690/ITSC-77-95
13. Organisation for Economic Co-operation and Development. (2018). *OECD due diligence guidance for responsible business conduct*. OECD Publishing. https://www.oecd.org/content/dam/oecd/en/publications/reports/2018/02/oecd-due-diligence-guidance-for-responsible-business-conduct_c669bd57/15f5f4b3-en.pdf
14. Veh, A., Göbel, M., & Vogel, R. (2019). Corporate reputation in management research: A review of the literature and assessment of the concept. *Business Research, 12*(2), 315–353. https://doi.org/10.1007/s40685-018-0080-4