# FROM CHECKLIST COMPLIANCE TO INTELLIGENCE-LED PREVENTION: A RISK-BASED FRAMEWORK FOR EFFECTIVE ANTI-MONEY LAUNDERING POLICY

**Azizbek Ilkhomzoda**
Tashkent International University
Xalqaro aloqalar departamenti hodimi
Email: azikilhom@gmail.com
ORCID: 0009-0009-3614-2944
https://doi.org/10.5281/zenodo.21358255

**ABSTRACT**

Money laundering transforms proceeds of crime into apparently legitimate assets and thereby protects the economic power of criminal organizations, corrupt officials, tax offenders, and other illicit actors. Yet anti-money-laundering systems often produce a paradox: regulated institutions generate millions of alerts and reports, while investigative authorities recover only a limited fraction of criminal proceeds. This thesis argues that the central policy problem is not an absolute shortage of compliance activity but a failure to allocate information and enforcement capacity according to risk. It develops an intelligence-led framework in which customer due diligence, beneficial-ownership transparency, transaction monitoring, suspicious-transaction reporting, supervision, investigation, prosecution, and asset recovery operate as an integrated information chain. The analysis distinguishes formal technical compliance from substantive effectiveness and explains why indiscriminate reporting, defensive de-risking, and uniform controls can reduce both financial inclusion and enforcement quality. It further examines emerging risks from virtual assets, digital payment systems, professional enablers, trade-based money laundering, and cross-border corporate structures. The thesis concludes that effective AML policy requires proportional controls, verified ownership information, interoperable databases, feedback from financial-intelligence units, specialized investigative capacity, and outcome-based evaluation. The objective should not be to maximize the number of reports filed, but to increase the probability that high-risk illicit flows are detected, disrupted, confiscated, and prevented without unnecessarily excluding legitimate users from the formal financial system.

**Keywords:** anti-money laundering; risk-based approach; beneficial ownership; financial intelligence; suspicious transaction reporting; asset recovery; financial inclusion.

**JEL Classification:** G28, K14, K22, K42, O17.

## 1. Introduction

Money laundering is not merely a technical banking offence. It is the financial infrastructure that allows predicate crimes to become durable economic power. When criminal proceeds can be stored, transferred, invested, and presented as legitimate wealth, the expected return to corruption, fraud, trafficking, cybercrime, tax crime, and organized violence rises. Laundering also damages lawful markets by enabling firms financed with criminal capital to underprice competitors, acquire strategic assets, influence public institutions, and conceal the real beneficiaries of transactions.

The estimated scale is necessarily uncertain because laundering is designed to remain hidden. UNODC continues to cite a broad estimate of two to five percent of global GDP, equivalent to hundreds of billions or trillions of dollars annually. The uncertainty itself is important: AML policy is conducted under severe informational constraints, and success

cannot be inferred from aggregate estimates or the simple volume of suspicious-transaction reports.

Modern AML systems place extensive obligations on banks, payment institutions, securities firms, insurers, casinos, real-estate professionals, lawyers, accountants, trust and company-service providers, and virtual-asset businesses. These obligations are necessary, but they can become ritualized. Institutions may demonstrate that forms were completed and alerts were reviewed without materially improving the identification of criminal networks. The resulting distinction is between technical compliance—whether rules and procedures exist—and effectiveness—whether illicit finance is actually detected, disrupted, prosecuted, and confiscated.

This thesis advances one central claim: AML should be understood as an information-allocation system. Every compliance requirement consumes scarce attention. If low-risk customers receive the same scrutiny as opaque companies, politically exposed persons, unusual cross-border structures, cash-intensive businesses, or rapidly moving virtual assets, the system creates noise that can hide the cases that matter most. A risk-based approach is therefore not a relaxation of enforcement. Properly designed, it is a method of concentrating verification, monitoring, investigation, and supervisory resources where the expected social loss is greatest.

## 2. Conceptual Foundations of Money Laundering

### 2.1 The laundering process

Money laundering is conventionally described through placement, layering, and integration. Placement introduces criminal proceeds into the financial or commercial system. Layering separates the assets from their origin through transfers, shell companies, nominees, false invoices, securities trades, crypto-asset swaps, or movement across jurisdictions. Integration returns the value to the beneficiary in a form that appears legitimate, such as business income, real estate, loans, dividends, or investment gains. Real cases do not always follow these stages sequentially, particularly when the predicate offence already occurs digitally or within the financial system, but the framework remains useful for identifying intervention points.

### 2.2 Economic and institutional harm

The harm from laundering extends beyond the concealment of a specific crime. Illicit financial flows can reduce tax revenue, distort competition, inflate asset prices, drain foreign exchange, weaken bank governance, and expose countries to abrupt losses of correspondent relationships. A financial institution may appear profitable while relying on deposits connected to opaque non-resident clients or high-risk intermediaries. When the underlying activity is exposed, legal penalties, liquidity pressure, reputational losses, and cross-border contagion can threaten financial stability.

AML policy also protects the credibility of public institutions. Corruption proceeds frequently move through companies whose legal owners are not their true beneficiaries. Without reliable beneficial-ownership information, procurement rules, conflict-of-interest restrictions, tax enforcement, sanctions, and asset-recovery procedures can all be circumvented. Transparency of ownership is therefore not an isolated corporate-law reform; it is an enabling condition for the wider integrity system.

## 3. The Risk-Based AML Architecture

### 3.1 From uniform controls to differentiated risk

The FATF Recommendations, as amended through October 2025, place the risk-based approach at the center of the global standard. Countries and regulated entities are expected to identify, assess, and understand their money-laundering and terrorist-financing risks and apply measures proportionate to those risks. This principle rejects two opposite errors: treating every customer as equally dangerous, and treating risk assessment as a justification

for weak controls. Enhanced measures should apply where risk is higher, while simplified measures may be appropriate where lower risk has been demonstrated.

A practical risk model combines customer risk, geographic risk, product risk, delivery-channel risk, transaction behavior, ownership opacity, and links to predicate offences. No single indicator should determine the outcome. A cash-intensive business is not inherently criminal; a politically exposed person is not presumed guilty; and a cross-border transfer is not suspicious merely because it is international. Risk emerges from combinations, inconsistencies, unexplained changes, and the absence of a credible economic purpose.

3.2 The AML information chain

An effective system can be represented as a chain: identification, verification, monitoring, reporting, analysis, investigation, adjudication, and confiscation. Customer due diligence establishes who is using the system and for what expected purpose. Beneficial-ownership verification determines who ultimately controls or benefits from a legal person or arrangement. Transaction monitoring compares actual behavior with the expected profile. Financial institutions report suspicious activity to a financial-intelligence unit, which combines private reports with government data, disseminates actionable intelligence, and provides feedback. Investigators then require legal authority, financial expertise, cross-border cooperation, and access to evidence. Prosecutors and courts convert intelligence into admissible proof, while asset-recovery authorities preserve and confiscate proceeds.

Weakness at any stage reduces the value of all previous stages. Perfect customer files are of limited use if reports disappear into an under-resourced FIU. Sophisticated analytics will fail if beneficial-ownership data are false. Strong investigations may still produce little deterrence if assets cannot be frozen quickly or if confiscation procedures are ineffective. AML reform should therefore diagnose bottlenecks across the complete chain rather than adding isolated obligations to the private sector.

**4. Why Checklist Compliance Underperforms**

4.1 Alert inflation and defensive reporting

Automated monitoring systems frequently generate large numbers of false positives. Institutions may adopt conservative thresholds because failing to report creates regulatory and reputational risk, whereas over-reporting imposes much of its cost on the FIU. This asymmetry encourages defensive reporting. The number of reports rises, but their average informational value falls. Investigators face a search problem in which genuinely important signals are buried within routine alerts.

The appropriate objective is not fewer reports in the abstract, but better-calibrated reports. Institutions need typologies, sector-specific indicators, network analytics, and feedback on which reports contributed to investigations. Supervisors should evaluate the reasoning, data quality, and escalation process behind reporting rather than rewarding volume. Feedback loops are critical because a reporting entity cannot improve if it never learns whether its alerts were useful.

4.2 De-risking and financial exclusion

When compliance costs and potential penalties are high, institutions may terminate entire categories of customers, jurisdictions, remittance providers, charities, or small businesses instead of managing risk individually. This practice, known as de-risking, can push legitimate transactions outside regulated channels and thereby reduce transparency. It can also raise remittance costs and disproportionately affect migrants, low-income households, non-profit organizations, and small firms.

The 2025 FATF revisions strengthened the emphasis on proportionality and financial inclusion. Tiered customer due diligence, lower-value accounts, digital identification, transaction limits, and progressive verification can bring lower-risk users into the formal system while preserving safeguards. Inclusion and integrity should not be treated as

opposites: formal participation can generate an auditable trail that cash-based exclusion does not.

**5. Priority Vulnerabilities**

5.1 Beneficial ownership and professional enablers

Shell companies and legal arrangements are attractive because they separate control from visible ownership. Registers are useful only when information is adequate, accurate, and up to date. Self-declaration without verification can transform a transparency reform into a database of untested claims. Effective systems combine company registries with tax records, identity databases, bank information, procurement data, and sanctions lists, while imposing proportionate liability for false filings and nominee abuse.

Lawyers, accountants, real-estate agents, company-formation agents, and other professional intermediaries can provide legitimate services that criminals exploit. Regulation must respect legal privilege and professional independence while ensuring that privilege does not protect participation in transactions, company formation, or asset concealment. Supervisory capacity outside the banking sector is often weaker even though these gatekeepers may design the structures later used by banks.

5.2 Digital finance and virtual assets

Digital payments create both risk and opportunity. High-speed transfers, remote onboarding, synthetic identities, mule accounts, decentralized protocols, mixers, privacy-enhancing tools, and cross-chain transactions can complicate tracing. At the same time, digital systems produce detailed data that can support graph analysis and rapid intervention. The policy task is to regulate entry and exit points, ensure travel-rule implementation where applicable, identify controlling persons, and promote cross-border access to time-sensitive information without assuming that every virtual-asset transaction is illicit.

5.3 Trade-based money laundering

Trade transactions can conceal value through over-invoicing, under-invoicing, multiple invoicing, false descriptions, phantom shipments, or deliberate mismatch between goods and payment flows. Detection requires information that banks alone may not possess. Customs data, shipping records, tax invoices, commodity prices, and corporate ownership information should be linked through risk analytics. Public-private cooperation is particularly important because relevant evidence is distributed across institutions and jurisdictions.

**6. An Outcome-Based Reform Framework**

A credible AML strategy should begin with a national risk assessment that identifies major predicate offences, sectors, products, geographic routes, and institutional weaknesses. The assessment should direct supervisory resources and should be periodically updated as risks evolve. Its purpose is not to produce a static report but to determine operational priorities, staffing, technology, and legislative reform.

Second, beneficial-ownership systems should move from collection to verification. Authorities should use automated cross-checks, risk flags, sanctions for false information, and mechanisms for regulated institutions to report discrepancies. Access rules must protect privacy while ensuring that competent authorities can retrieve information rapidly.

Third, FIUs and investigative bodies need analytical and technological capacity equal to the reporting burden imposed on the private sector. Structured reporting formats, unique identifiers, network analysis, link analysis, and secure information exchange can increase the value of collected data. Specialized financial investigators should be integrated into major corruption, fraud, organized-crime, cybercrime, and tax investigations from the beginning rather than added after the proceeds have moved.

Fourth, supervision should measure effectiveness. Useful indicators include the proportion of high-risk entities receiving risk-based inspections, remediation of identified weaknesses, timeliness and quality of suspicious-transaction reports, intelligence

disseminations that lead to investigations, successful parallel financial investigations, restraint and confiscation of assets, international cooperation, and reduction of recurrent typologies. These measures should be interpreted carefully, because an increase in detected cases may initially indicate stronger enforcement rather than more crime.

Finally, enforcement must be proportionate and credible. Minor documentation failures should not receive the same response as deliberate facilitation, repeated systemic weakness, concealment of beneficial owners, or failure to act on clear red flags. Personal accountability may be justified for senior managers who knowingly permit serious breaches, while institutions that disclose problems, cooperate, and remediate should face a different response from those that obstruct supervision.

**7. Policy Matrix**

| Weakness | Risk created | Priority reform | Outcome indicator |
|---|---|---|---|
| Unverified ownership data | Anonymous control of companies and assets | Cross-database verification and discrepancy reporting | Share of high-risk entities with verified ultimate owners |
| Excessive low-quality alerts | Important signals buried in noise | Calibrated monitoring and FIU feedback | Reports converted into actionable intelligence |
| Uniform customer treatment | High cost and financial exclusion | Tiered and proportionate due diligence | Formal access preserved with controlled residual risk |
| Weak non-bank supervision | Displacement toward gatekeepers and cash-intensive sectors | Risk-based supervision of DNFBPs | Coverage and remediation in high-risk sectors |
| Fragmented public data | Slow investigations and missed networks | Secure interoperable analytics | Time required to trace ownership and freeze assets |
| Low confiscation capacity | Crime remains profitable | Early financial investigation and asset management | Value restrained and finally confiscated |

**8. Implications for Uzbekistan and Emerging Economies**

Emerging economies face a dual challenge: strengthening financial integrity while expanding formal finance, investment, remittances, and digital payments. Uzbekistan's AML/CFT framework was assessed by the Eurasian Group in 2022, and the IMF's 2025 Financial Sector Assessment described the regime as largely effective while emphasizing the need to address remaining weaknesses. Continued progress should focus on effectiveness, particularly beneficial-ownership verification, risk-based non-bank supervision, quality of financial intelligence, parallel financial investigations, cross-border cooperation, and asset recovery.

Rapid digitalization makes proportionality especially important. Excessively burdensome onboarding can preserve cash dependence, while weak onboarding can facilitate mule accounts and identity abuse. A tiered framework linked to transaction limits, reliable digital identity, behavioral monitoring, and enhanced review when risk increases can support both inclusion and integrity. Regional cooperation is also essential because illicit flows

rarely respect national borders and may exploit differences in company law, customs controls, virtual-asset regulation, and investigative capacity.

## 9. Conclusion

Anti-money laundering policy succeeds only when information collected for compliance becomes intelligence that changes criminal incentives. Expanding rules, forms, alerts, and penalties can create the appearance of strictness while leaving the main laundering channels intact. The alternative is an intelligence-led, risk-based system that verifies ownership, differentiates risk, connects private and public data, provides feedback, investigates finances alongside predicate crimes, and confiscates proceeds.

The appropriate measure of success is therefore not the quantity of compliance activity. It is the increased probability that serious illicit flows are identified and disrupted, that criminal assets are recovered, and that lawful users remain inside transparent financial channels. Effective AML is not maximal surveillance of everyone; it is disciplined concentration on the persons, structures, transactions, and networks that present the greatest demonstrable risk.

## References

1. Basel Institute on Governance. (2024). Basel AML Index 2024. Basel Institute on Governance.
2. FATF. (2012–2025). International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations. Paris: Financial Action Task Force.
3. FATF. (2014). Guidance for a Risk-Based Approach: The Banking Sector. Paris: Financial Action Task Force.
4. FATF. (2021). Guidance on Risk-Based Supervision. Paris: Financial Action Task Force.
5. FATF. (2023). Beneficial Ownership and Transparency of Legal Persons. Paris: Financial Action Task Force.
6. FATF. (2025). Guidance on Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion. Paris: Financial Action Task Force.
7. Ferwerda, J. (2009). The economics of crime and money laundering: Does anti-money laundering policy reduce crime? Review of Law & Economics, 5(2), 903–929.
8. IMF. (2023). Review of the Fund's Anti-Money Laundering and Combating the Financing of Terrorism Strategy. Washington, DC: International Monetary Fund.
9. IMF. (2025). Republic of Uzbekistan: Financial Sector Assessment Program. Washington, DC: International Monetary Fund.
10. Levi, M., Reuter, P., & Halliday, T. (2018). Can the AML system be evaluated without better data? Crime, Law and Social Change, 69, 307–328.
11. Pol, R. F. (2020). Anti-money laundering: The world's least effective policy experiment? Policy Design and Practice, 3(1), 73–94.
12. Reuter, P., & Truman, E. M. (2004). Chasing Dirty Money: The Fight Against Money Laundering. Washington, DC: Institute for International Economics.
13. Sharman, J. C. (2011). The Money Laundry: Regulating Criminal Finance in the Global Economy. Cornell University Press.
14. Takáts, E. (2011). A theory of "crying wolf": The economics of money laundering enforcement. Journal of Law, Economics, & Organization, 27(1), 32–78.
15. UNODC. (2011). Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes. Vienna: United Nations Office on Drugs and Crime.