The American Journal of Political Science Law and Criminology
ISSN 2693-0803 Volume 08 - 2026

Digital transformation in the activities of the Department for Combating Economic Crimes, serving as the national Financial Intelligence Unit (FIU)

Azizbek Khalmurzayev
Master's Student, Law Enforcement Academy of the Republic of Uzbekistan

Received: 28 Feb 2026 | Received Revised Version: 16 Mar 2026 | Accepted: 04 Apr 2026 | Published: 30 Apr 2026

Volume 08 Issue 04 2026 | Crossref DOI: 10.37547/tajpslc/Volume08Issue04-09

Abstract

Digital transformation of Financial Intelligence Units (FIUs) is examined as a strategic transition from a "document-driven workflow" to a managed flow of risk signals. This involves machine-readable formats for Suspicious Transaction Reports (STRs), automated data quality validation, risk scoring, and traceable routing of intelligence materials. The empirical part of the study details the implementation of the Department's "Markaz" software, designed for the ranking, processing, and analysis of STRs. Furthermore, it outlines the mechanism for automated cross-referencing against specific categories, including terrorist watchlists, wanted persons, and inquiries from foreign FIUs.

Keywords: Financial Intelligence Unit (FIU), AML/CFT/CPF (Anti-Money Laundering / Countering the Financing of Terrorism / Countering the Financing of the Proliferation of Weapons of Mass Destruction), Digital Transformation, Risk Assessment Center (RAC), Suspicious Transaction Report (STR), Risk Scoring and Ranking, "Markaz" Information System, Actionable Intelligence, Interoperability.

Cite This Article: Azizbek Khalmurzayev. (2026). Digital transformation in the activities of the Department for Combating Economic Crimes, serving as the national Financial Intelligence Unit (FIU). The American Journal of Political Science Law and Criminology, 8(04), 52–55. https://doi.org/10.37547/tajpslc/Volume08Issue04-09

1. Introduction

In the global economy, capital flows faster than ever before, while money laundering schemes evolve with equal velocity. Under these circumstances, the effectiveness of Financial Intelligence Units (FIUs) can no longer rely solely on "manual" analysis and human resources. The exponential growth in the volume of Suspicious Transaction Reports (STRs) inevitably drives the system toward end-to-end automation—from data ingestion to the dissemination of materials to law enforcement agencies. As noted in FATF analytical reviews, mature FIUs are transitioning from reactive information processing to a model centered on risk prioritization and data analytics.

In accordance with the Decree of the President of the Republic of Uzbekistan No. UP-6252 dated June 28, 2021, the Risk Assessment Center (RAC) was established within the structure of the Department for Combating Economic Crimes under the General Prosecutor's Office of the Republic of Uzbekistan. The Center serves as the "core" for risk-oriented analysis and technological modernization, as well as an analytical hub in the field of Anti-Money Laundering, Countering the Financing of Terrorism, and Countering the Financing of the Proliferation of Weapons of Mass Destruction (AML/CFT/CPF). Such institutionalization of analytical functions aligns with international best practices, where, according to the Egmont Group, strategic analytics is viewed as a key driver of the national financial

intelligence system's effectiveness.

The operational model of the Risk Assessment Center (RAC) is built upon three interconnected pillars.

The first is analytics, which encompasses typological research and strategic analysis. This involves identifying new and evolving schemes for money laundering and terrorism financing, detecting trends and anomalies in financial behavior, and utilizing automated tools for Big Data analysis. As Professor Michael Levi notes, modern financial intelligence must shift from mere analysis toward the proactive detection of criminal activity.

In a practical sense, this signifies a transition from fragmented studies to a systemic "scanning" of flows and risk signals.

The second pillar is risk assessment. The RAC (Risk Assessment Center) coordinates the activities of state bodies and organizations responsible for AML/CFT/CPF, ensures the implementation of risk assessments, and is empowered with regulatory and rulemaking functions. Thus, the focus is not merely on processing incoming signals but on "setting the rules of the game": defining which risks are prioritized, how they are measured, and how they are integrated into the regulatory framework.

According to World Bank experts, the integration of National Risk Assessment (NRA) into regulatory mechanisms is precisely what defines the maturity of an AML/CFT system. This allows for the transformation of analytical findings into practical regulatory decisions.

The third pillar is technological implementation. The RAC is responsible for integrating advanced information technologies into the AML/CFT/CPF framework, including the development of software products and ensuring the rapid exchange of information among all participants of the national "anti-money laundering" system. This is a pivotal point: digital transformation here is not merely an "add-on" but the core infrastructure that integrates primary monitoring, supervision, and the law enforcement block into a single operational circuit.

The FATF methodology emphasizes that technological infrastructure must facilitate a continuous analytical cycle—from data acquisition to the generation of actionable intelligence.

Pursuant to Clause 12 of the Decree of the President of the Republic of Uzbekistan No. UP-6252, the Department’s proprietary software product, "Markaz" (translated as "The Center"), was implemented. This system is designed to automate the ranking, processing, and analysis of Suspicious Transaction Reports (STRs) within the AML/CFT/CPF framework. Experts estimate that the integration of intelligent STR processing systems significantly enhances the efficiency of detecting high-risk operations without increasing the workload on Financial Intelligence Unit (FIU) personnel.

The logic of this system is based on end-to-end automation through the following stages:

Receipt and primary processing of STRs;

Analytical processing and formulation of findings;

Dissemination of analytical results to executors for "implementation";

An interaction platform for inquiries, feedback, and communication with supervisory authorities and the private sector.

This interconnectedness is particularly crucial considering the "starting point": prior to the launch of the "Markaz" system, the process operated in a semi-automatic mode, which objectively hindered the timeliness of analysis and the referral of materials to law enforcement agencies for legal action. The transition to an automated cycle essentially transforms STRs from a "document flow" into a stream of managed signals with clear priorities and traceable actions.

As noted in OSCE research, digital analytical platforms shift the work of financial intelligence from document processing to the management of financial risk flows.

Technology cannot function effectively without unified data standards and procedures. Consequently, the regulatory framework governing STR submissions has been concurrently strengthened. Specifically, the Resolution of the Cabinet of Ministers of the Republic of Uzbekistan No. 402, dated June 29, 2021, established the procedure for submitting STRs. Furthermore, the updated STR reporting form was approved by an Order of the Head of the Department, registered by the Ministry of Justice of the Republic of Uzbekistan on February 7, 2023, under Registration No. 3419.

From the FATF perspective, data standardization is a critical factor in ensuring the interoperability of information systems among all participants within the AML/CFT/CPF framework..

По сути, это «правовая сборка» цифрового контура: когда у участников единые форматы и единый порядок, автоматизация становится не локальной инициативой, а системным режимом работы.

In analytics, a simple rule prevails: the quality of findings depends on the quality of the input data. As previously noted, improvements began at the "foundation"—the process of receiving, collecting, and processing STRs. Transitioning to secure channels and machine-readable formats reduces the reliance on manual entry and mitigates the risk of technical errors.

The next layer of maturity involves automated logical controls. The system is capable of rejecting reports with incorrect fields (for instance, an erroneous TIN or date) and returning them to the reporting entity for correction. This fundamentally transforms data discipline: "input errors" are not propagated through the chain but are eliminated at the point of origin.

The core mechanism of the "Markaz" system is automated ranking—a risk assessment process where each incoming STR is assigned a risk score based on specific indicators. Subsequently, STRs are prioritized into three levels: high (red), medium (yellow), and low (green). This approach aligns with the international trajectory for the digital transformation of FIUs: moving from basic automation toward advanced analytics (AI/ML) and Big Data processing (Business Intelligence/BI).

The ranking process incorporates a set of practice-oriented criteria:

- Type of transaction and suspicion category;
- Frequency and volume of transactions;
- Geographical location of the participant/counterparty;
- Geographical location of the participant's/counterparty's bank;
- Alignment with previously identified typologies of money laundering, terrorism financing (ML/TF), and predicate offenses.

In practical terms, this signifies a "shift in workload" from human to algorithm (machine): specialists concentrate on high-risk cases rather than expending significant time on analyzing repetitive reports. Crucially, the prioritization logic is based on indicators and typologies—knowledge accumulated through analytics and risk assessment—rather than abstract statistics.

Another vital function is the processing of STRs based on monitored categories of persons, featuring automated cross-referencing against:

- Subjects of parallel financial investigations;
- Individuals on national and international terrorist watchlists;
- Subjects of inquiries from foreign FIUs;
- The list of wanted persons.

It is specifically noted that the dissemination of lists concerning persons linked to terrorism or the proliferation of weapons of mass destruction (WMD) to reporting entities is carried out automatically via "Markaz," in strict adherence to FATF requirements. This functionality is integrated with UN Security Council resources, ensuring automated updates of lists and user notifications through the "Markaz" personal account dashboard.

To summarize the described approach in a single thesis: the digital transformation of the FIU represents a transition from "reacting to reports" to managing risks in a continuous-flow mode. The established RAC aligns methodology (typologies and risk assessment), the regulatory framework (STR procedures and forms), and the technological environment (the "Markaz" system), where data is controlled at entry, risks are measured automatically, and inter-agency cooperation becomes part of a unified process.

2. Conclusion

Global practice demonstrates that the effectiveness of financial intelligence is determined by the ability to integrate analytics, technology, and inter-agency cooperation into a unified process. The establishment of the RAC and the implementation of the "Markaz" system underscore the Republic of Uzbekistan's transition toward an analytically oriented FIU model, where risk management serves as the central element of operations.

The synergy of the regulatory framework, analytical methodology, and digital solutions forms a resilient infrastructure for detecting financial crimes. In an era of accelerating digitalization of financial flows, the further evolution of analytical tools and technological

integration will determine the resilience of the national system and its effectiveness in countering emerging threats in the field of AML/CFT/CPF and predicate offenses.

References

1. Financial Action Task Force (FATF). Методология оценки соответствия Рекомендациям ФАТФ и эффективности систем ПОД/ФТ (Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems). – FATF, Париж.
2. Egmont Group of Financial Intelligence Units. Principles for Information Exchange and Operational Guidance for Financial Intelligence Units. – Egmont Group Secretariat.
3. Levi M. Money Laundering and Its Regulation: A Critical Analysis // Journal of Money Laundering Control. – исследования типологий финансовых преступлений и аналитических подходов.
4. World Bank. National Risk Assessment and AML/CFT Framework Development Guidance. – World Bank Group.
5. Financial Action Task Force (FATF). Методология оценки соответствия Рекомендациям ФАТФ и эффективности систем ПОД/ФТ (Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems). – FATF, Париж.
6. Arner D., Barberis J., Buckley R. The Evolution of RegTech and SupTech in Financial Services // Journal of Financial Transformation.
7. OECD. Digital Transformation and Data Analytics in Public Sector Governance and Financial Supervision. – Organisation for Economic Co-operation and Development.
8. Financial Action Task Force (FATF). Международные стандарты по противодействию отмыванию денег, финансированию терроризма и распространению оружия массового уничтожения (Рекомендации ФАТФ). – FATF.
9. FATF/Egmont Executive Summary (PDF): https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Digital-Transformation-executive-summary.pdf