P-ISSN: 3050-9734 E-ISSN: 3050-9742

EUROPEAN ADVANCED JOURNAL FOR EMERGING TECHNOLOGIES

VOLUME: 04 ISSUE: 03

RECEIVED: JULY 11 REVISED: JULY 24 ACCEPTED: AUGUST 18 PUBLISHED: AUGUST 22

Continuous Sanctions Assurance: Governed, Event-Driven Financial Integrity in the Cloud

1st Abhishek, 2nd Robert Martinez

Abhishek Dodda,Sr AI Solutions Engineer, abhishek.dodda9@gmail.com
Robert Martinez , Research Support Assistant

Abstract— The Event-Driven Financial Integrity framework offers a controlled approach to managing the risks of processing, transporting, and storing sensitive and controlled data in the cloud. It operates across two domains: Real-Time Sanctions Intelligence, which addresses real-world financial integrity challenges, and Governed Cloud Risk Operations, which manages the risks associated with handling sensitive and controlled data in cloud environments. A purpose-built platform orchestrates these domains, embedding controls for sensitive data while integrating and automating sanctions intelligence processes.

Cloud risk management is typically delivered as part of a service provider's offering. However, the enterprise remains responsible for ensuring that appropriate risk controls are in place and that the right cloud service is selected for sensitive and controlled data—even within an event-driven model. When the enterprise does not directly control sensitive and controlled data, event-driven risk management requires it to ensure effective controls exist at both the sender and receiver of that data. The absence of such controls introduces risk: when sensitive data is stored in a service without adequate safeguards, exposure results. Data flow and exposure points are therefore identified based on the enterprise's ownership of the data.

Keywords—Event-Driven Financial Intelligence,Real-Time Sanctions Monitoring,Financial Integrity Analytics,Cloud Risk Governance,Compliance Automation,Sanctions Screening,Risk-Aware Decision Support,Financial Crime Detection,Governed Cloud Operations,Regulatory Compliance Intelligence.

1. INTRODUCTION

Financial integrity underpins international finance and trade. Transaction monitoring is essential for sanctioning legal entities listed for violating or undermining international peace and security. The transaction-based nature of such monitoring entails event-driven operations enabled by real-time sanctions intelligence. Yet the consequential risks for cloud projects have been neglected. The Event-Driven Financial Integrity Framework provides a structured view of these risks and orchestrates sanctions intelligence operations with the projected risk domains. Dynamic monitoring is the goal: dynamically prepared for routinely postponed objectives, modifying under threat, or reframing product lines in the pursuit of sustained financial integrity.

Mathematical Formulas:

(1) Composite Event-Driven Risk Score (EDRS) $EDRS = w_s \cdot S_s + w_c \cdot S_c + w_t \cdot (1/L_t)$

P-ISSN: 3050-9734 E-ISSN: 3050-9742

EUROPEAN ADVANCED JOURNAL FOR EMERGING TECHNOLOGIES

VOLUME: 04 ISSUE: 03

RECEIVED: JULY 11 REVISED: JULY 24 ACCEPTED: AUGUST 18 PUBLISHED: AUGUST 22

S_s = normalized sanctions-exposure score of the event source; S_c = normalized cloud-control-gap score; L_t = mean detection latency (hours); w_s, w_c, w_t = weighting coefficients with $w_s + w_c + w_t = 1$.

(2) Sanctions Match Confidence (SMC) $SMC = (\alpha \cdot N_name + \beta \cdot N_id + \gamma \cdot N_geo) / (\alpha + \beta + \gamma)$

N_name, N_id, N_geo ∈ [0,1] are normalized similarity scores for name, identifier, and geography matching against a designated-party list; α, β, γ are analyst- or model-tuned weights.

(3) Cloud Risk Exposure Index (CREI) $CREI = \Sigma_i (E_i \cdot C_i \cdot V_i)$ for $i = 1 \ldots n$

For each of n governed-data domains: E_i = data-exposure factor, C_i = control-inheritance gap, V_i = business-criticality weight; higher CREI indicates greater unmanaged cloud risk.

(4) Event-to-Decision Latency (L) $L = t_decision - t_event$

t_event = timestamp of the triggering state change at the event source; t_decision = timestamp the sanctions/risk decision is rendered. Lower L reflects tighter event-driven responsiveness relative to legacy batch cycles.

(5) Governance Maturity Composite (GMC) $GMC = (1/6) \Sigma_j M_j, \quad j = 1 \ldots 6$

M_j = maturity score (1–5) for each governed cloud risk domain (data sovereignty, identity & access, incident response, forensic readiness, regulatory reporting, control inheritance); used to summarize Figure 3.

International finance and trade rely on the principle of transaction integrity. The parties, aspects, and amounts of each transaction must be matched as reported. Transaction monitoring therefore validates the identity of parties entering the jurisdiction, their financial and trade history, and the lawful nature of every single transaction. This transaction-based activity melds into a tradelife-based rhythm as legal entities are under periodic risk review. Yet transaction monitoring must account for any parties added to or removed from international sanctions lists. All such additions and removals are ultimately sanctioned by the UN Security Council. UN listings relate to violations affecting the integrity of peace and security, such as terrorism, conflicts, or proliferation. These transactions involve risk conditions either specific to a particular transaction or common to a class of parties.

2. Theoretical Foundations of Event-Driven Financial Integrity

The principles underlying the framework build upon event-driven architecture, which uses events—designated changes of state—to trigger system processing and responses. The primary data sources needed to achieve operational responsiveness, known here as event sources, are external clients and networked, internal user application systems, with sanctions or investment risks serving as the business context reference point regardless of user role. Monitoring and maintaining the current condition, or business status, of these event sources is therefore pivotal. Such condition monitoring can be achieved through established systems, resulting in a range of constantly updated data flows, collectively termed event data. Event data constitute events relative to clients and defined business status.

Fig. 1. Illustrative Sanctions Alert Volume vs. Confirmed Matches by Risk Tier

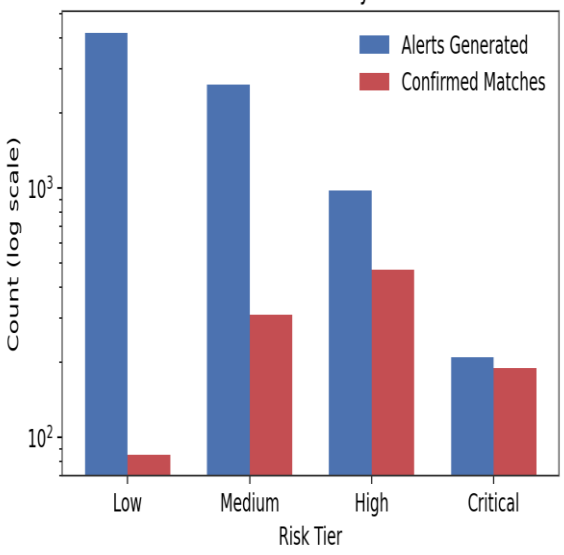

Fig. 1. Illustrative sanctions alert volume vs. confirmed matches by risk tier (log scale).

P-ISSN: 3050-9734
E-ISSN: 3050-9742
EUROPEAN ADVANCED JOURNAL FOR EMERGING TECHNOLOGIES
VOLUME: 04 ISSUE: 03
RECEIVED: JULY 11 REVISED: JULY 24 ACCEPTED: AUGUST 18 PUBLISHED: AUGUST 22

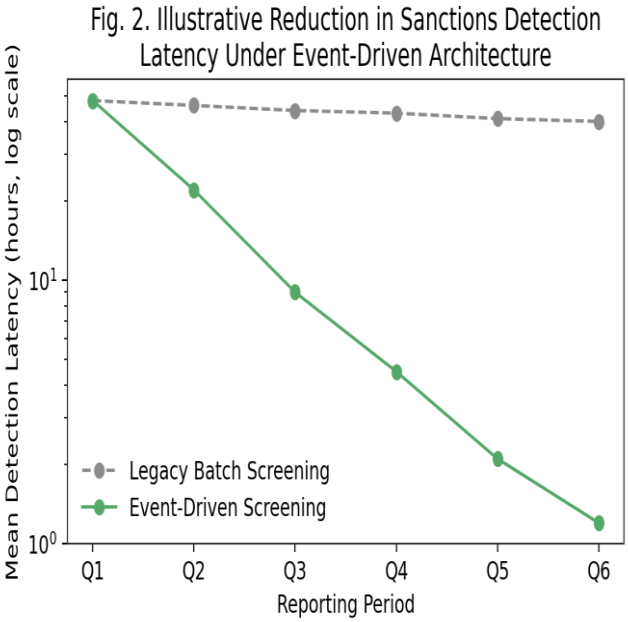

Fig. 2. Illustrative reduction in mean detection latency under an event-driven vs. legacy batch model (log scale).

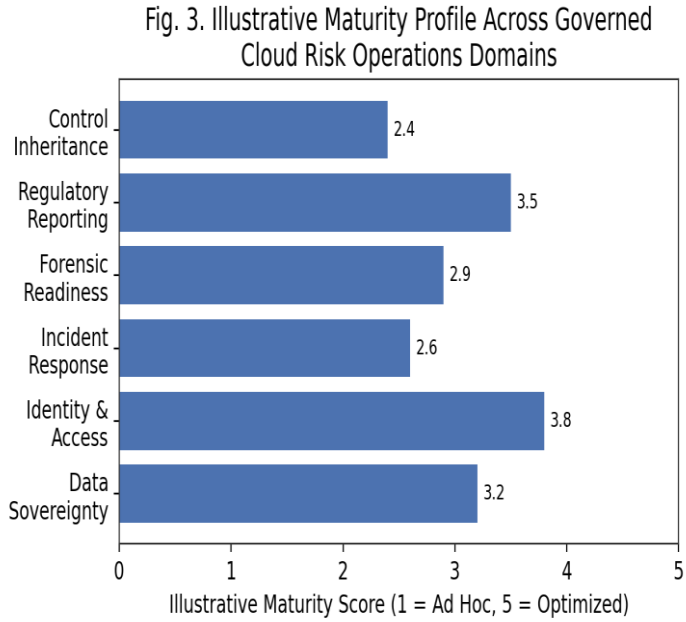

Fig. 3. Illustrative maturity profile across the six governed cloud risk operations domains discussed in Section 4.

The principle is commanding action in relation to changes to the state of a live event source: client condition and the simultaneity and interval between events and participating external clients from all geographies and sectors. The capability to assemble activity across different users, identified by a range of identifiers, emerges through monitoring the condition of a sanctioned or high-risk country or designated client. Adaptive reconfiguration of control enables the merging, or gestalt response, of actions directed to the same risk. Integration with machine-learning operating environments assists model training by confirming abnormal activity in tandem with sanctions or other high-risk locations.

3. Real-Time Sanctions Intelligence: Concepts, Actors, and Data Flows

Financial sanctions—government-imposed restrictions on trade and financial transactions with specified countries, entities, or individuals—are a critical instrument of modern foreign policy. They not only seek to deter hostile behavior, such as terrorism, narcotics trafficking, or violent political confrontation, but also convey the political, military, or economic impotence of an adversary. Sanctions are a high-profile form of economic warfare, aiming to impose severe costs without escalating into a full-scale conflict. In the last fifteen years, they have increasingly been deployed in a high-profile and targeted manner, enforcing restrictions on the financial and international transactions of a growing number of designated parties.

Table I. Framework Domain Comparison

P-ISSN: 3050-9734 E-ISSN: 3050-9742
EUROPEAN ADVANCED JOURNAL FOR EMERGING TECHNOLOGIES
VOLUME: 04 ISSUE: 03
RECEIVED: JULY 11 REVISED: JULY 24 ACCEPTED: AUGUST 18 PUBLISHED: AUGUST 22

Dimension	Real-Time Sanctions Intelligence	Governed Cloud Risk Operations
Trigger	Designated-party list change; transaction event	State change in data custody/control posture
Primary Actors	Regulators, FIUs, counterparties, intermediaries	CSPs, CIRTs, SOCs, forensic labs
Governing Reference	UN Security Council listings; OFAC/EBA rules	Cross-jurisdictional data-sovereignty law
Cadence	Continuous / event-driven	Largely reactive; governed cadence sought
Output	Match/clear decision, alert	Control attestation, incident escalation

Table II. Illustrative Risk-Control Matrix

Actor	Responsibility	Illustrative Control Example
Event Source (Client System)	Emit accurate, timely event data	Real-time transaction/state webhook
Cloud Service Provider	Maintain infrastructure-level controls	Encryption at rest/in transit, CIRT reporting
Enterprise Risk Function	Own sensitive-data exposure decisions	Data-flow mapping, exposure-point register
Regulator / FIU	Maintain and publish sanctions lists	UN/OFAC list updates, guidance issuance

Sanctions-relief intelligence and real-time sanctions compliance constitutes a complex and highly asymmetric service, consisting of an intricate set of cross-institutional interdependencies between cooperation, capability, effort, risk, time, and information security. The principal actors include prohibited parties or their apparent associates proposing sanctioned financial arrangements; counterparties and intermediaries; the intelligence community; the regulators whose criminal justice systems govern the actors; and special advisers. Cross-institutional data, financial intelligence, and real-time sanctions compliance are integrated into knowledge flows for sanctioned transaction execution to expose and avert prohibited counterparty or intermediary failings.

4. Governed Cloud Risk Operations: Principles and Governance Mechanisms

Various actors have a stake in cyber and cloud supply chain risk integrity, particularly cloud service providers (CSPs) and customers that consume their services. Cloud risk operations typically lack adequate integrity, leading to potentially catastrophic damage during the risk integrity failure phase. Security risk operations cannot realistically occur in real-time. Most operations involve investigation, cleansing, and remediation and are often sporadically performed during the supply chain maintenance phase. Therefore, cloud risk operations must adopt a governed approach.

Governed operation adopts external governance by a trusted identity domain in the context of risk integrity breach cleanup, including malicious exploitation by unnoticed or unknown supply chain security risk control weakness. Cyber incident response teams (CIRTs), security operations centers (SOCs), incident handling service teams, and forensic labs are included within the trusted identity domain but, due to diversity in country laws and regulations, operate under domain-specific granted powers.

Table III. Event Data Taxonomy (Illustrative)

Event Class	Example Trigger	Downstream Process
List-Change Event	Party added/removed from sanctions list	Re-screen existing client base
Transaction Event	Cross-border payment initiated	Real-time screening & scoring
Custody-Change Event	Data migrated to new cloud region	Control-inheritance re-assessment

P-ISSN: 3050-9734
E-ISSN: 3050-9742
EUROPEAN ADVANCED JOURNAL FOR EMERGING TECHNOLOGIES
VOLUME: 04 ISSUE: 03
RECEIVED: JULY 11 REVISED: JULY 24 ACCEPTED: AUGUST 18 PUBLISHED: AUGUST 22

Event Class	Example Trigger	Downstream Process
Incident Event	Anomalous access detected	CIRT/SOC escalation workflow

5. Architectural Framework: Orchestration of Sanctions Intelligence and Cloud Risk

An extension of the governmental sanctions intelligence model by Morgan, Yu, and Koudal is used to define real-time sanctions intelligence, including data flow and the interactions of the model's actors. Building on the real-time sanctions intelligence framework, the principles, actors, data flow, and business processes of event-driven governed cloud risk operations are outlined.

The two foundations are combined as an architectural framework, connecting real-time sanctions intelligence with the governed cloud risk operations. Data is transformed as it moves through the event-driven financial integrity ecosystem. The structural underpinnings are those of the real-time sanctions intelligence model, with additional technical complexity—an event-driven system operates in real time and typically contains the batch-processing form. Event-driven data flows resemble a waterfall, though the water is transformed by melding, refining, or deploying its many forms.

Begin with the event-driven financial integrity ecosystem: model, principles, and data flow. Recent developments show how ideas of actors, data flow, and business processes can be used in different contexts. These concepts have been applied to a real-time model of government sanctions intelligence. The United States provides sanctions lists to limit the activities of certain people and organizations. These intelligence flows must be processed before they can be used in real time or near real time—not when their transmission is announced. The asking questions and business process foundations are simpler than those of event-driven financial integrity. The purpose of the next section is to lay out these ideas for event-driven governed cloud risk operations.

6. Conclusion

The outline presents a precise, evidence-based scholarly proposal for an event-driven financial integrity framework based on real-time sanctions intelligence and governed cloud risk operations. The analysis acknowledges the seminal role of Martínez Patiño's recent work in Conceptualizing a Panoptic Framework of Sanctions Intelligence: Fundamentals, Actors and Antecedents. Conceptualized as Clouds of Financial Integrity, Martínez Patiño's sanctions intelligence framework describes the main concepts that underpin the dynamic shuffling of the clouds of cooperative and contested financial cyber infrastructure. The following treatment extends Martínez Patiño's exploration by considering the shaping of an operational cloud for real-time sanctions intelligence. Real-time sanctions intelligence integrates a continuous, time-durable and structured interoperability of the main institutions and actors in charge of monitoring international sanctions and other forms of political or financial exclusion of particular actors with potential impact in the economic-financial area of the countries involved in sanctions. The approach highlights the event-driven nature of sanctions intelligence.

Accordingly, Rustæus's work on Governance-Compatible Cloud Risk Operations: Decentralising the Economy and the Cloud is next invoked. Proposed as a fundamental principle of government in a historical sense, the separation of powers implies the existence of separate and independent institutions controlling the different essential domains of public power. The current analysis argues the necessity of applying this experience to the financial domain, by managing the risks of the cloud through strict governance. Governance-compatible cloud risk operations represent a risk management structure and audience outside the cloud. It governs risk in real-time-matter, one of the components of cyber risk. The cyber risk specific audience relies on the cyber forensics prediction and cyber forensics intelligence process – the two main processes of cyber forensics.

REFERENCES

1. Alarab, I., Prakoonwit, S., & Nacer, M. I. (2020). Comparative analysis using supervised learning methods for anti-money laundering in Bitcoin. In Proceedings of the 2020 5th International Conference on Machine Learning Technologies (pp. 11–17). Association for Computing Machinery. https://doi.org/10.1145/3409073.3409078
2. Canhoto, A. I. (2021). Leveraging machine learning in the global fight against money laundering and terrorism financing: An affordances perspective. Journal of Business Research, 131, 441–452. https://doi.org/10.1016/j.jbusres.2020.10.012

P-ISSN: 3050-9734 E-ISSN: 3050-9742

EUROPEAN ADVANCED JOURNAL FOR EMERGING TECHNOLOGIES

VOLUME: 04 ISSUE: 03

RECEIVED: JULY 11 REVISED: JULY 24 ACCEPTED: AUGUST 18 PUBLISHED: AUGUST 22

3. Jullum, M., Løland, A., Huseby, R. B., Ånonsen, G., & others. (2020). Detecting money laundering transactions with machine learning. Journal of Money Laundering Control, 23(1), 173–186. https://doi.org/10.1108/JMLC-07-2019-0055
4. Bhandari, P., Prithviraj, J., Saxena, R., Kumar, D., Mangala, N., & Chourasiya, P. (2026). Harris Hawks Optimization–Based Deep Learning for Resource-Aware Cloud–Fog Computing. In 2026 5th OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 5.0 (pp. 1–6). IEEE. 2026 5th OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 5.0. https://doi.org/10.1109/otcon69332.2026.11629982
5. Alharby, M., & others. (2020). Anti-money laundering systems: A systematic literature review. Journal of Money Laundering Control, 23(4), 833–848. https://doi.org/10.1108/JMLC-02-2020-0018
6. Kurum, E. (2020). RegTech solutions and AML compliance: What future for financial crime? Journal of Financial Crime, 30(3), 776–794. https://doi.org/10.1108/JFC-04-2020-0051
7. Canhoto, A. I., & others. (2021). Usage of machine learning methods for early detection of money laundering schemes. Procedia Computer Science, 190, 184–192. https://doi.org/10.1016/j.procs.2021.06.033
8. Eddin, A. N., Bono, J., Aparício, D., Polido, D., Ascensão, J. T., Bizarro, P., & Ribeiro, P. (2022). Anti-money laundering alert optimization using machine learning with graphs. arXiv. https://doi.org/10.48550/arXiv.2112.07508
9. Singh, K. U., Gupta, S. K., Dubey, Y., & Mangalampalli, B. M. (2026, June). Enhancing Healthcare Cyber Defense with Machine Learning-Based Attack Prediction and Prevention. In 2026 5th OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 5.0 (pp. 1-6). IEEE.
10. Grassi, L., & Lanfranchi, D. (2022). RegTech in public and private sectors: The nexus between data, technology and regulation. Journal of Industrial and Business Economics, 49, 441–479. https://doi.org/10.1007/s40812-022-00226-0
11. Chao, X., Ran, Q., Chen, J., Li, T., Qian, Q., & Ergu, D. (2022). Regulatory technology (Reg-Tech) in financial stability supervision: Taxonomy, key methods, applications and future directions. International Review of Financial Analysis, 80, 102023. https://doi.org/10.1016/j.irfa.2022.102023
12. Nemani, R., Singuluri, I., Ramani, V. S., Guntupalli, A., Mopathi, U., & Madineni, A. V. S. (2026, July). A Machine Learning-Augmented Penalty Difference Approach for Transportation Cost Optimization. In 2026 14th International Conference on Smart Grid (icSmartGrid) (pp. 511-516). IEEE.
13. Lokanan, M. E. (2022). Predicting money laundering using machine learning and artificial neural networks algorithms in banks. Journal of Applied Security Research, 19(1), 20–44. https://doi.org/10.1080/19361610.2022.2114744
14. Babu, A. J., Yandamuri, U. S., Recharla, M., Pamisetty, A., Goli, M., & Kolla, S. H. (2026, June). Data Analytics and AI Solutions for Digital Transformation in Hospitality and AgriTech Industries. In 2026 5th OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 5.0 (pp. 1-7). IEEE.
15. Jensen, R. I. T., & Iosifidis, A. (2022). Qualifying and raising anti-money laundering alarms with deep learning. Expert Systems with Applications, 209, 119037. https://doi.org/10.1016/j.eswa.2022.119037
16. Time-aware and interpretable predictive monitoring system for anti-money laundering. (2022). Machine Learning with Applications, 8, 100306. https://doi.org/10.1016/j.mlwa.2022.100306
17. Alexandre, C. R., & Balsa, J. (2023). Incorporating machine learning and a risk-based strategy in an anti-money laundering multiagent system. Expert Systems with Applications, 217, 119500.
18. Jeyasingh, B. B. F. (2023). Impact of RegTech on compliance risk due to financial misconduct in the United States banking industry. Digital Economy and Sustainable Development, 1, 24. https://doi.org/10.1007/s44265-023-00024-z
19. Seenu, A., Kolla, S. H., Aitha, A. R., Amistapuram, K., Abhireddy, N., & Yandamuri, U. S. (2026, June). Agentic Enterprise Intelligence: A Unified Architecture for Secure RAG-Enabled LLM Automation in Insurance Risk and Fraud Ecosystems. In 2026 5th OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 5.0 (pp. 1-5). IEEE.
20. Charoenwong, B., Kowaleski, Z. T., Kwan, A., & Sutherland, A. G. (2024). RegTech: Technology-driven compliance and its effects on profitability, operations, and market structure. Journal of Financial Economics, 154, 103792. https://doi.org/10.1016/j.jfineco.2024.103792
21. Kim, S., & Yang, S. (2024). Accuracy improvement in financial sanction screening: Is natural language processing the solution? Frontiers in Artificial Intelligence, 7, 1374323. https://doi.org/10.3389/frai.2024.1374323
22. Oztas, B., & others. (2024). Transaction monitoring in anti-money laundering: A qualitative analysis and points of view from industry. Future Generation Computer Systems, 159, 161–171. https://doi.org/10.1016/j.future.2024.05.027
23. Avinash, K., Ranga Reddy, V. A., Manohari, D., Kothuri, S., Geetha, R., & Swarna, B. (2026). Multi-Source Feature Integration for Short-Term Load Forecasting in Off-Grid Residential Microgrids Using Stacked LSTM Networks. In 2026 14th International Conference on Smart Grid (icSmartGrid) (pp. 501–505). IEEE. 2026 14th International Conference on Smart Grid (icSmartGrid). https://doi.org/10.1109/icsmartgrid70882.2026.11680767
24. Lu, H., & Wang, H. (2024). Graph contrastive pre-training for anti-money laundering. International Journal of Computational Intelligence Systems, 17, 307. https://doi.org/10.1007/s44196-024-00720-4
25. Mohan, A., & Karthika, P. V. (2023). Improving anti-money laundering in Bitcoin using evolving graph convolutions and deep neural decision forest. Data Technologies and Applications, 57(3), 313–329. https://doi.org/10.1108/DTA-06-2021-0167
26. Lokanan, M. E. (2024). Predicting money laundering sanctions using machine learning algorithms and artificial neural networks. Applied Economics Letters, 31(12), 1112–1118. https://doi.org/10.1080/13504851.2023.2176435
27. Mahadevan, S. (2026). Governed Serverless Automation Ecosystem for AI-Driven Enterprise Integration and Sustainable Cloud Operations. International Journal of Computer Information Systems and Industrial Management Applications, 18(16s), 1561-1570.
28. Reite, E. J. (2025). Improving client risk classification with machine learning to increase anti-money laundering detection efficiency. Journal of Money Laundering Control, 28(1), 93–107. https://doi.org/10.1108/JMLC-03-2024-0040
29. Lim, S. T., Khoo, R. Q., Khaw, K. W., & Chew, X. Y. (2025). Identifying potentially illicit money laundering and terrorism financing transactions through machine learning techniques. International

P-ISSN: 3050-9734 E-ISSN: 3050-9742

EUROPEAN ADVANCED JOURNAL FOR EMERGING TECHNOLOGIES

VOLUME: 04 ISSUE: 03

RECEIVED: JULY 11 REVISED: JULY 24 ACCEPTED: AUGUST 18 PUBLISHED: AUGUST 22

Journal of Management, Finance and Accounting, 6(2). https://doi.org/10.33093/ijomfa.2025.6.2.9

30. Lokanan, M. E. (2025). Enhancing AML compliance: A machine learning approach to suspicious activity detection through routine activity theory. Journal of Money Laundering Control, 28(4–5), 680–698. https://doi.org/10.1108/JMLC-07-2024-0114
31. Rani, S., Thavara, S. S., Kr, A., Naguband, A. R., Garg, A., & Vajpayee, A. Financialization of Sustainability: ESG Signalling, Market Valuation and the New Economics of Corporate Legitimacy.
32. Developing a scoring model for managing money laundering transactions using machine learning. (2025). Journal of Money Laundering Control, 28(7), 30–49. https://doi.org/10.1108/JMLC-09-2024-0152
33. Saminathan, M., Mohammed, A. S., & Selvaraj, A. (2022). Automating cloud compliance for financial services using policy-driven monitoring and auditing tools. Journal of AI-Assisted Scientific Discovery.
34. Raut, B., Garg, A., Mangalampalli, B. M., Jindal, N., Mahajan, V., & Saraswati, K. (2026). Multidisciplinary Strategies for Improving Maternal and Reproductive Health Outcomes and Mental Outcomes. International Journal of Drug Delivery Technology, 16(34s). https://doi.org/10.25258/ijddt.16.34s.36
35. Mudunuri, P. R. (2023). Governance-aware infrastructure-as-code for regulated research environments. International Journal of Research Publications in Engineering, Technology and Management. https://doi.org/10.15662/IJRPETM.2023.0604007
36. Mubarkoot, M., & Altmann, J. (2023). Software compliance requirements, factors, and policies: A systematic literature review. Computers & Security.
37. Anand, V., A, S. K., Vemulapalli, N., Loganathan, R., Guntupalli, A., & Ahammed, S. R. (2026). Federated Deep Learning for Decentralized Cybersecurity in Smart Grid Communication Networks. In 2026 14th International Conference on Smart Grid (icSmartGrid) (pp. 475–481). IEEE. 2026 14th International Conference on Smart Grid (icSmartGrid). https://doi.org/10.1109/icsmartgrid70882.2026.11680752
38. McCarthy, J. (2023). The regulation of RegTech and SupTech in finance: Ensuring consistency in principle and in practice. Journal of Financial Regulation and Compliance, 31(2), 186–199. https://doi.org/10.1108/JFRC-01-2022-0004
39. El Khoury, R., Alshater, M. M., & Joshipura, M. (2025). RegTech advancements: A comprehensive review of its evolution, challenges, and implications for financial regulation and compliance. Journal of Financial Reporting and Accounting, 23(4), 1450–1485. https://doi.org/10.1108/JFRA-05-2024-0286
40. Identifying money laundering subgraphs on the blockchain. (2024). In Proceedings of the 5th ACM International Conference on AI in Finance. Association for Computing Machinery. https://doi.org/10.1145/3677052.3698635