



Generative Intelligence for Fraud-Proof Wealth and Compliance

1st Venkata krishna azith ganti , 2nd Luca Romano

Venkata Krishna Azith Teja Ganti, Sr Data Support Engineer , venkatakrishna.azith.de@gmail.com
Luca Romano , Graduate Research Assistant

Abstract— This work presents a Generative Financial Intelligence Framework designed to strengthen fraud resistance in wealth management and detect compliance violations related to Anti-Money Laundering (AML) and Counter Financing of Terrorism (CFT) obligations. The framework comprises four core components: (1) data architecture, (2) anomaly detection and risk scoring, (3) fraud-resistant wealth management, and (4) synthetic data and scenario generation. Each component is grounded in Principal-Agent Theory and designed to comply with relevant financial regulations, governance standards, and supervisory expectations.

Generative Financial Intelligence is defined here as an enterprise's capability to generate auxiliary, data-driven models from internal and external knowledge sources to support decision-making. These models serve dual purposes: understanding and improving enterprise operations, and predicting future behaviors of the enterprise or its stakeholders. This concept extends beyond the definition of Financial Intelligence established by the Association of Certified Financial Crime Specialists (ACFCS), by augmenting predictive capabilities derived from internal data with auxiliary data sourced from both private-sector and public-domain channels.

Keywords—Generative Financial Intelligence, Fraud-Resistant Wealth Management, Financial Fraud Detection, Regulatory Compliance, Generative Artificial Intelligence, Anti-Money Laundering, Financial Risk Analytics, Intelligent Decision Support, Wealth Management Analytics, Compliance Intelligence.

1. INTRODUCTION

Generative Financial Intelligence is defined as a data-driven mechanism that infers insights into the behaviour of stakeholders from historical records; generates synthetic yet plausible scenarios of future stakeholders' behaviour; and ultimately informs decision-making and control processes. The decision supporting capabilities of Generative Financial Intelligence distinguish it from its traditional counterpart. Generative Financial Intelligence conveys the capability to deploy statistical and simulation models to create rich generative probabilistic models—one for each data source or for different grouping of data sources and type of behaviour—because the behaviour of the stakeholders of interest can be effectively summarised in different feature spaces. In practice, the generative behaviour modelling stage can be divided in two parts: the definition of behaviour types and a generative modelling phase, which uses the behaviour type definitions to feed dedicated generative models. Both capabilities can be exploited to support stakeholders' fraud detection mechanisms using machine learning classifiers and anomaly detection based on reconstruction errors. Generative Financial Intelligence thus enables a bank's Fraud Control Unit to better monitor its clients from both fraud-resistance and compliance-boosting perspectives.

The adoption of Generative Financial Intelligence enables the integration of data coming from different, disconnected sources in a unified way, removing the need to create complex and expensive data pipelines involving the directly observable behaviour and the approximation with a generative model. The probabilistic nature of the output of the Generative Financial Intelligence framework also means that stakeholders can explore Natural Language Generate-, Image-, or Sound-based people-, event- and scenario-based models to do it in a fully data-driven way—without relying on the tentative imaginations and assumptions of employees or external consultants.

Table I. Core Components of the Generative Financial Intelligence Framework



#	Component	Primary Function	Aligned Theory / Standard
1	Data Architecture	Integrates 1st/2nd/3rd-party and synthetic data sources	Data governance & lineage standards
2	Anomaly Detection & Risk Scoring	Flags multi-dimensional deviations; computes client risk index	Principal-Agent Theory
3	Fraud-Resistant Wealth Management	Controls over withdrawals, transfers, high-risk transactions	FCA five-driver strategy
4	Synthetic Data & Scenario Generation	Produces plausible adversarial/non-factual test scenarios	AML/CFT supervisory expectations

Table II. Data Source Taxonomy

Category	Description	Illustrative Examples
First-party	Directly observed client transactions and holdings	Account transfers, portfolio holdings, login activity
Second-party	Client-generated activity from partnered channels	Sentiment from client-linked social feeds
Third-party	External context data from vendors/processors	Stripe/PayPal aggregate flows, crypto-funding signals
Synthetic	Model-generated plausible-but-non-factual scenarios	Simulated fraud gestures, adversarial test cases

A. Compliance and Regulatory Alignment

Compliance with applicable financial regulations, governance standards, and supervisory expectations is a cornerstone of fraud-resistant wealth management and compliance decision-making systems. Transparency, fairness, and accountability are normative objectives that require the financial interests of stakeholders—including clients, employees, investors, and society at large—to be protected from breaches of trust, public disclosure, treatment as second-class citizens, and reputational damage. Such

objectives demand that institutions identify beneficial and harmful behaviours, document controls over bad behaviours, and assess product and service tampering against integrity-assured conditions. Rich information bases enable compliance teams to perform these tasks without incurring excessive resource burdens.

Generative financial intelligence aims to meet these needs. It enables compliance teams to see beyond the sometimes deceptive, non-realistic outlooks of sentiment analysis, social media reputation modelling, and forensic investigations. By supporting the generation of synthetic but internally consistent scenarios, it empowers teams to examine difficult-to-detect behaviours across the three lines of defence, from business-as-usual activities to rarer incidents to testing over the longer term. However, the normalisation of fraud-resistant monitoring responses is essential for implementation in practice without additional resource drain and distraction. Nonetheless, fraud losses are often reimbursed by companies, as required by banking and insurance regulation, e.g., in the EU. To that end, messages from control detection teams that have been trained for pluriannual periods have to be supported by continuous explanation and justification-based anticipatory risk-scaling adaptation from lines of defense horizontal centers.

Table III. Four-Grade Risk Scoring Scale

Grade	Score Range	Trigger	Escalation Action
Low	0 - 25	Routine variance within baseline	Passive monitoring, no action
Medium	26 - 50	Moderate deviation from client profile	Analyst review within SLA
High	51 - 75	Pattern consistent with known fraud typology	Case opened; second-line escalation
Critical	76 - 100	Multi-signal convergence / regulatory relevance	Immediate freeze & compliance referral



Table IV. Fraud-Resistant Wealth Management Decision Workflows

#	Workflow	Control Objective
1	Threshold-based fund movement checks	Identify withdrawals/transfers above defined limits
2	Accounting transaction review	Detect prominent-risk transaction subcategories
3	Consolidated client risk assessment	Link fund routing to a comprehensive client risk score
4	Revenue-significant transaction linkage	Tie high-revenue transactions to entity risk score
5	Manual approval mapping	Map B2B collection/payment approvals to requester risk score

2. Conceptual Foundations

Generative Financial Intelligence is delineated as a data-driven inference, synthetic scenario generation, and decision-support capability that extends the concept of financial intelligence. It combines characteristics of financial analysts and artificial intelligence to achieve objectives aligned with financial sector regulations, governance frameworks, and supervisory expectations. Distinctive aspects of Generative Financial Intelligence include data provenance, model robustness, decision-logic interpretability, ethical safeguards, privacy protection, and communication intelligibility for monitoring and decision-making teams.

Generative Financial Intelligence encompasses three core capabilities: (i) the ability to identify multi-dimensional anomalies in factual datasets that are indicative of unusual conditions, events, or trends, and therefore deserve scrutiny as potential risks; (ii) the generation of adversarial examples that are plausible, yet non-factual, thereby challenging the organization's assumptions, biases, or decisions; and (iii) the contextualization of any signal or scenario detection and the associated risk scoring within the perspectives of trust, reputation, and compliance, to facilitate risk detection, assessment, and management. Such capabilities serve as foundations for the fraud-resistant mechanisms.

Fig. 1. Generative Financial Intelligence architecture: data flows from source integration through anomaly

detection/risk scoring into fraud-resistant controls and compliance decisioning.

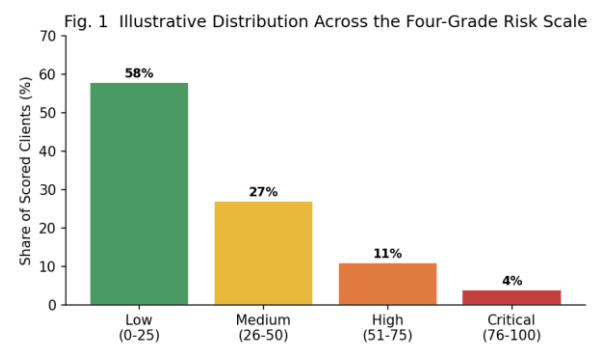
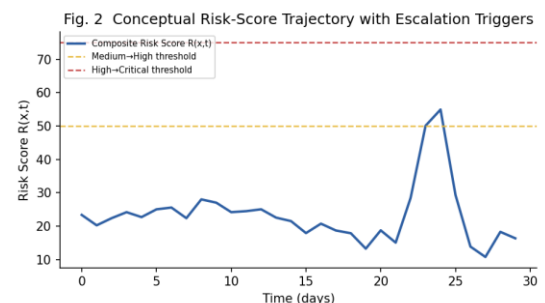


Fig. 2. Illustrative distribution of scored clients across the four-grade risk scale.



A.

Definitions of Generative Financial Intelligence

Generative Financial Intelligence is defined as the set of information-processing capabilities that support security and privacy-oriented risk decisions across financial crime, fraud, and compliance domains. Such decisions can be informed using a Generative Financial Intelligence system that addresses the following objectives. (i) for a given initial set of data and an associated data-collection roadmap, detect anomalous user behavior that has a high probability of being associated with illicit activity; (ii) score users according to their illicit insider-fringe risk level and trigger escalations for risk-based monitoring mechanisms using fraud detection teams that are organized according to the three lines of defense model; (iii) calibrate the aforementioned risk indicators through historical analyses; and (iv) complement anomaly-detection workflow results by identifying past instances of similar detection outcomes and their business impact.



Central components of the Generative Financial Intelligence Framework are adaptable data-driven anomaly detection and risk-scoring decisions. Such mechanisms are fraud-resistant when their indices are considered in the context of a well-structured control architecture, as exemplified by a Generative Financial Intelligence roadmap for closing-loop financial fraud systems, i.e., financially loss-making situations, and achieving decision-making fraud resistance in financial companies delivering products and services to individuals through their websites.

Fig. 3 Generative Financial Intelligence Architecture (conceptual flow)



Fig. 3. Conceptual trajectory of a composite risk score over time, crossing Medium→High and High→Critical escalation thresholds.

3. Methodological Framework

The research adopts a qualitative, exploratory approach: within the context of a senior-capstone project, a Generative Financial Intelligence Framework is constructed to support fraud-resistant wealth and compliance decisions, building upon theoretical groundwork for Generative Financial Intelligence. The design addresses stakeholder needs, meets UK regulatory and supervisory expectations, adheres to legislation and standards concerned with data ethics and privacy, and employs systematic data-management procedures. The framework's individual components remain operationally independent yet are designed to function as a cohesive system, enhancing fraud resistance and regulatory compliance across the three dimensions of people, processes, and technology.

Compliance with the Financial Services and Markets Act 2023 and wider data regulations is central to the framework. The following solution design and evaluation criteria reflect the five drivers set forth by the Financial Conduct Authority

in its latest strategy for the UK financial-services sector — delivering strong consumer and market outcomes, being resilient and sustainable, enabling a competitive market landscape with fair outcomes for consumers, embracing innovation and technological change, and supporting the FCA's mission to make financial markets work well for people. These criteria place added emphasis on people and processes, specifically the design of technology to bolster staff decision-making and supervision and enable more-frequent detection of misconduct.

A. Data Architecture and Sources

Data provenance and recency have an important bearing on a Generative Financial Intelligence Framework's efficacy and relevance. Financial datasets are highly complex and use case specific. These characteristics necessitate the cataloguing of various sources that can be harnessed for fraud-resistant wealth management and compliance decisions, along with accompanying data ingestion infrastructure to ensure ongoing, timely updates and appropriate data lineage checks. Dedicated auxiliary data streams can further enhance fraud detection capabilities by adding context around anomalous behaviour.

Input data for detection, scoring and profiling processes naturally derives from user transactions and holdings (first-party data). Supplementary feeds also drawn from user activities (e.g., sentiment analysis of recent tweets) would ideally calibrate thresholds for scoring abnormal events. Anomalous detections could then trigger targeting via custom-designed credit card offers, travel deals, or ad banners. Third-party data (e.g., large-scale transaction analysis from Stripe or PayPal) would provide valuable external context and also inform era-defining abnormal behaviour. Other rich sources of external data that bear relevance to trade analysis and risk appetites of key user segments (e.g., crypto funding activity of high-net-worth individuals in Latam) should also be considered.

Mathematical Formulas:

1. Reconstruction-error anomaly score

$$A(x) = \|x - \hat{x}\|^2 \quad (1)$$

where x is the observed feature vector and $\hat{x}$ is its reconstruction from the generative model; larger $A(x)$ indicates a stronger anomaly signal.



2. Composite client risk score

$$R(x) = \sum_i w_i \cdot f_i(x), \quad \sum_i w_i = 1 \quad (2)$$

where $f_i(x)$ are normalised risk features (e.g., anomaly score, transaction severity, historical dishonesty) and w_i are weights set by the control architecture.

3. Grade assignment (escalation mapping)

Grade(x) = Low if $R(x) < 26$; Medium if $26 \leq R(x) < 51$; High if $51 \leq R(x) < 76$; Critical if $R(x) \geq 76$ (3)

a piecewise mapping of the continuous risk score onto the four-grade scale in Table III.

4. Compliance risk index (AML/CFT weighting)

$$C(x) = \alpha \cdot R(x) + \beta \cdot S(x) \quad (4)$$

where $S(x)$ is a synthetic-scenario plausibility score from adversarial example generation, and α, β calibrate the relative weight of observed versus simulated risk.

4. Fraud-Resistant Wealth Management Mechanisms

The architecture of Generative Financial Intelligence is enriched by mechanisms that promote fraud-resistant decisions in wealth management, assisting in the management of prominent fraud risks spanning client-funds-securing interfaces, accounting transactions, comprehensive risk assessments, significant-risk transactions, and crucial operational roles. These mechanisms substantially enhance the fraud-resistance attributes of wealth-management decisions at distinct cost centres while facilitating regulatory compliance—thus, they constitute a meaningful upgrade to the existing financial and operational-support systems.

Five key decision workflows are fortified by requisite control planes. The decisioning-support functionalities do not impose a dependency on Generative Financial Intelligence, yet they furnish supplementary assurances of fraud resilience and compliance with applicable regulatory mandates: (1) identification of client fund withdrawals, transfers, or employs service transactions that fall above entities' defined threshold limits; (2) detection of accounting transactions with underlying scenarios that involve prominent-risk subcategories; (3) linking of all above-mentioned properties to a consolidated risk assessment of the use and routing of

client funds, thereby confirming suitability for generating a comprehensive risk score for the client; (4) identification of transactions classified under any service category that contribute significantly towards the entities' overall revenue and linking of such transactions to the risk score of the routing entity; and (5) detection of manual approval requests seeking B-B collections and payments in order to correctly map these relations to the approved status and the risk score of the requesting party.

A. Anomaly Detection and Risk Scoring

Anomaly detection constitutes a foundational capability for overcoming fraud resistance gaps in traditional financial intelligence systems. A variety of techniques are available, catering to diverse operational needs, with specific algorithms delivering optimal performance for particular data signatures. To align with control requirements associated with financial fraud, plausible techniques must be identified and applied across suitable datasets. These encompass supervised, semi-supervised, and unsupervised methods, and are tasked with addressing specific anomaly classes, such as known fraud patterns, evolving fraud gestures and species, or emerging fraud mechanisms. Attention to appropriate feature selection and rigorous model calibration offer further potential to enhance detection fidelity, while black box explainability enables issuance of highly intelligible and interpretable alerts and warnings.

A numerical risk scoring framework serving risk-monitoring functions supports anomaly detection capabilities by assessing the likelihood of sudden spikes in recent operational activities. More sophisticated than simple thresholds, the risk scales leverage features, control points, and fraud-resistance coverage patterns across the primary fraud classes detected, deploying a four-grade scale to highlight the risk level, triggers, and escalation processes that facilitate proactive risk governance. Continuous adoption adaptive control angles enable the scale to address dynamic operational conditions.

5. Conclusion

By delineating a Generative Financial Intelligence Framework that applies AI technologies to the governance of economic crime and regulatory compliance, this work enables wealth-management decisions that are more resistant



to fraud while remaining aligned with applicable laws and regulations. These capabilities are structured behind an architectural foundation consisting of requisite data sources, models, control planes, and decision workflows, allowing users to proactively manage Financial Intelligence Act (FIA) compliance obligations and detect criminal activities within their financial services. A specific example is the detection of potential fraudsters applying for loans guaranteed by insurance agencies, but the framework offers a broad crime-governance capability.

As with any research, practical armamentarium, or policy decision, these instruments are not infallible. They create a higher degree of automatic verification in a high-fraud-risk environment, offering instructions on who can be flagged at the application stage. Yet, as past experience has repeatedly demonstrated, people's desires can be stronger than the fear of consequences; therefore, a certain level of fraud will occur despite the best controls put in place. The next logical step is to use the same types of data to establish an overall risk scoring of clients over time to consider their past level of dishonesty and the risk of moving them to a less controlled area of the business without active monitoring.

REFERENCES

- Al-Hashedi, K. G., & Magalingam, P. (2021). Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019. *Computer Science Review*, 40, Article 100402.
- Ali, A., Razak, S. A., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., & Nasser, M. (2022). Financial fraud detection based on machine learning: A systematic literature review. *Applied Sciences*, 12(19), Article 9637.
- Bender, E. M., Gebru, T., McMillan-Major, A., & Shmitchell, S. (2021). On the dangers of stochastic parrots: Can language models be too big? In *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency* (pp. 610–623).
- Mashetty, S. (2024). Leveraging Deep Learning, Neural Networks, and Data Engineering for Intelligent Mortgage Loan Validation: A Data-Driven Approach to Automating Borrower Income, Employment, and Asset Verification. *Neural Networks, and Data Engineering for Intelligent Mortgage Loan Validation: A Data-Driven Approach to Automating Borrower Income, Employment, and Asset Verification* (December 21, 2024).
- Bommasani, R., Hudson, D. A., Adeli, E., Altman, R., Arora, S., von Arx, S., Bernstein, M. S., Bohg, J., Bosselut, A., Brunskill, E., Brynjolfsson, E., Buch, S., Card, D., Castellon, R., Chatterji, N., Chen, A., Creel, K., Davis, J. Q., Demszky, D., ... Liang, P. (2021). On the opportunities and risks of foundation models. *arXiv*.
- European Parliament and Council of the European Union. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*.
- KOLLA, S. K. (2024). DEEP LEARNING AND CLINICAL NLP FRAMEWORK FOR AUTOMATED KNOWLEDGE EXTRACTION FROM MULTIMODAL HEALTH . TPM – Testing, Psychometrics, Methodology in Applied Psychology, 31(S2), 134–140. Retrieved from <https://tpmap.org/submission/index.php/tpm/article/view/4748>
- Hernandez Aros, L., Bustamante Molano, L. X., Gutierrez-Portela, F., Moreno Hernandez, J. J., & Rodríguez Barrero, M. S. (2024). Financial fraud detection through the application of machine learning techniques: A literature review. *Humanities and Social Sciences Communications*, 11, Article 1130.
- Hilal, W., Gadsden, S. A., & Yawney, J. (2022). Financial fraud: A review of anomaly detection techniques and recent advances. *Expert Systems with Applications*, 193, Article 116429.
- Rohit Gorle. (2024). Deep Learning Approaches for Threat Detection in Multi-Cloud Environments. *Journal of Computational Analysis and Applications (JoCAAA)*, 33(07), 3857–3864. Retrieved from <https://eudoxuspress.com/index.php/pub/article/view/5879>
- International Monetary Fund. (2023). Generative artificial intelligence in finance: Risk considerations. *IMF Fintech Notes*, 2023(006).
- Kapoor, D., & Bhatia, A. (2024). A comprehensive study on generative AI risks in the financial sector: Challenges and solutions. *Journal of Harbin Engineering University*, 45(3), 303–311.
- Organisation for Economic Co-operation and Development. (2023). Generative artificial intelligence in finance. *OECD Artificial Intelligence Papers*, No. 9.
- Manukonda, K. R. R. (2024). Chapter-5 Enhancing Test Automation Efficiency Through AI-driven Reporting: An Empirical Study on Defect Detection and Resolution Time. *ADVANCES IN*, 119, 107.
- Otubu, R. O. (2024). Integrating generative AI in fraud detection and anti-money laundering: A comprehensive review and framework proposal. *Journal of Emerging Trends in Engineering and Applied Sciences*, 15(5).
- OpenAI. (2023). GPT-4 technical report. *arXiv*.
- Ouyang, L., Wu, J., Jiang, X., Almeida, D., Wainwright, C., Mishkin, P., Zhang, C., Agarwal, S., Slama, K., Ray, A., et al. (2022). Training language models to follow instructions with human feedback. *Advances in Neural Information Processing Systems*, 35, 27730–27744.
- Yandamuri, U. S. (2024). AI-Driven Decision Support Systems for Operational Optimization in Hospitality Technology. *Metallurgical and Materials Engineering*.
- Weidinger, L., Mellor, J., Rauh, M., Griffin, C., Uesato, J., Huang, P.-S., Cheng, M., Glaese, A., Balle, B., Kasirzadeh, A., et al. (2021). Ethical and social risks of harm from language models. *arXiv*.
- Gunasekaran, R. M. N. (2024). Generative AI: Opportunities, risks and implications for financial services. *The Eastasouth Journal of Information System and Computer Science*, 1(3).
- National Institute of Standards and Technology. (2023). Artificial intelligence risk management framework (AI RMF 1.0) (NIST AI 100-1).
- Movva, V. R. (2024). Cloud-Native Platform Engineering for High-Scale Retail Systems: Designing Resilient Microservices and Intelligent Infrastructure. Available at SSRN 7449480.
- Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bannetot, A., Tabik, S., Barbado, A., García, S., Gil-López, S., Molina, D., Benjamins, R., et al. (2020). Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion*, 58, 82–115.



24. Zhao, W. X., Zhou, K., Li, J., Tang, T., Wang, X., Hou, Y., Min, Y., Zhang, B., Zhang, J., Dong, Z., et al. (2023). A survey of large language models. arXiv.
25. Manukonda, K. R. R., Swamy, H., Sankar, R., & CM, C. (2024, August). Application of Explicit Group Sparse Projection in Optimizing 5G Network Resource Allocation and Topology Design. In 2024 4th Asian Conference on Innovation in Technology (ASIANCON) (pp. 1-6). IEEE.
26. Dwivedi, Y. K., Kshetri, N., Hughes, L., Slade, E. L., Jeyaraj, A., Kar, A. K., Baabdullah, A. M., Koohang, A., Raghavan, V., Ahuja, M., et al. (2023). So what if ChatGPT wrote it? Multidisciplinary perspectives on opportunities, challenges and implications of generative conversational AI for research, practice and policy. *International Journal of Information Management*, 71, Article 102642.
27. Feuerriegel, S., Hartmann, J., Janiesch, C., & Zschech, P. (2024). Generative AI. *Business & Information Systems Engineering*, 66, 111–126.
28. Bommasani, R., et al. (2021). On the opportunities and risks of foundation models. arXiv.
29. Shabsigh, G., & Boukherouaa, E. B. (2023). Generative artificial intelligence in finance: Risk considerations. *IMF Fintech Notes*, 2023(006).
30. Mangalampalli, B. M. Intelligent Data Profiling for Healthcare Data Lakes Using AI-Enhanced Analytics.
31. Financial Action Task Force. (2021). Opportunities and challenges of new technologies for AML/CFT.
32. Financial Action Task Force. (2021). Updated guidance for a risk-based approach to virtual assets and virtual asset service providers.
33. Mahadevan, S. (2024). Empowering Manufacturing: Generative AI Revolutionizes ERP Application. *Int. J. Innov. Sci. Res*, 9, 593-595.
34. Financial Action Task Force. (2022). Targeted update on implementation of the FATF standards on virtual assets and virtual asset service providers.
35. Financial Action Task Force. (2023). Targeted update on implementation of the FATF standards on virtual assets and virtual asset service providers.
36. Yandamuri, U. S. (2022). Cloud-Based Data Integration Architectures for Scalable Enterprise Analytics. *International Journal of Intelligent Systems and Applications in Engineering*, 10, 472-483.
37. Financial Action Task Force. (2024). Targeted update on implementation of the FATF standards on virtual assets and virtual asset service providers.
38. Basel Committee on Banking Supervision. (2021). Principles for the effective management and supervision of climate-related financial risks. Bank for International Settlements.
39. Mangalampalli, B. M. Generative AI Applications In Healthcare Data Mart Design And Optimization.
40. Basel Committee on Banking Supervision. (2021). Principles for operational resilience. Bank for International Settlements.
41. Financial Stability Board. (2024). The financial stability implications of artificial intelligence.
42. Bank for International Settlements. (2021). Artificial intelligence and machine learning in financial services: Market developments and financial stability implications.
43. European Banking Authority. (2021). EBA report on the use of digital platforms in the EU banking and payments sector.
44. European Banking Authority. (2023). Follow-up report on the use of machine learning for internal ratings-based models.
45. Mahadevan, S., Desani, N. R., Yadav, P. S., Joseph, T., & Malcom, A. (2024). FutureTech Innovations. Cari Journals USA LLC.
46. International Organization of Securities Commissions. (2021). The use of artificial intelligence and machine learning by market intermediaries and asset managers.
47. International Organization of Securities Commissions. (2024). Artificial intelligence in capital markets: Use cases, risks, and challenges.