

## Proposed PhD Research Outline

### Provisional Title: Machine Learning–Based Internal Fraud Risk Scoring in Banking Using Enterprise Risk Registers: A Continuous Monitoring Framework

Prepared by: Ibrahim Olalekan Usman

#### 1.0 Motivation and Background

Internal fraud remains a persistent and material source of operational risk in banking, contributing to financial losses, reputational damage, and regulatory sanctions (Supriyadi, Priyarsono and Andati, 2023). While banks have adopted various governance and control mechanisms to mitigate insider threats, internal fraud continues to evolve alongside increasing digitalisation, complex IT infrastructures, and distributed operational processes (Supriyadi, Priyarsono and Andati, 2023; Oko-Odion and Angela, 2025). In practice, many financial institutions rely on enterprise IT and operational risk registers to document insider incidents, control weaknesses, mitigation actions, and residual risks. These registers contain rich, structured historical data, yet they are typically used for *static, periodic risk assessments rather than predictive or continuous risk intelligence* (Quinn et al., 2024; Bonet et al., 2021).

Traditional internal fraud risk assessment approaches rely heavily on expert judgement, qualitative scoring matrices, and simplified formulas such as  $\text{Risk} = \text{Probability} \times \text{Impact}$  (Beckley, 2025). Although these methods are practical and auditable, they lack statistical rigour, dynamic updating, and early-warning capability, particularly in environments where fraud patterns change rapidly (Ilori et al., 2024). Recent studies have demonstrated the effectiveness of machine learning techniques, *particularly Extreme Gradient Boosting (XGBoost)*, in detecting internal fraud by capturing non-linear relationships and complex interactions within financial data (Supriyadi, Priyarsono and Andati, 2023).

However, from a practitioner’s perspective, *my professional experience working with Tier-1 African banks reveals that fraud detection models are often model-centric and static, deployed as one-off analytical solutions without continuous monitoring, governance integration, or systematic updating*. Risk monitoring remains largely manual or reactive, despite the availability of structured risk register data that could support automated and forward-looking risk scoring. This gap between analytical capability and operational deployment motivates this research.

This PhD aims to transform existing “strict monitoring” practices for internal fraud by Supriyadi, Priyarsono and Andati in 2023 into a machine learning–enabled, continuously monitored, and explainable risk scoring framework, grounded in Enterprise Risk Registers (ERR) and aligned with regulatory expectations for transparency, auditability, and model risk management.

#### 2.0 Literature Context and Research Gap

Recent research on internal fraud detection in banking has increasingly adopted machine learning techniques, including decision trees, ensemble models, and gradient boosting methods (Temuçin, 2025; Supriyadi, Priyarsono and Andati, 2023). In particular, XGBoost has demonstrated strong performance in internal fraud classification due to its ability to manage class imbalance and capture complex, non-linear feature interactions. Complementary studies highlight the value of unsupervised anomaly detection approaches, such as Isolation Forests, for identifying emerging or previously unseen fraud patterns in environments where labelled fraud data is limited or incomplete (Ski, 2024).

Parallel work in financial risk modelling has emphasised the importance of model risk, stability, and interpretability, especially when models inform operational, compliance, or governance decisions within regulated institutions. Recent contributions stress that poorly governed models can introduce significant model risk, even when predictive accuracy appears strong (Lazar, Qi and Tunaru, 2024). In response, the growing MLOps literature demonstrates that continuous monitoring, automated retraining, feature governance, and explainability mechanisms are critical to maintaining model reliability, auditability, and regulatory compliance once machine learning models are deployed in production environments (Daramola, Chy and Fonkem, 2025).

Despite these advances, internal fraud risk within banks remains inadequately modelled using Enterprise Risk Register (ERR) data. In practice, internal fraud risks, such as insider misuse of access, control circumvention, and system abuse, are still assessed using static Probability  $\times$  Impact matrices embedded within risk registers. These approaches lack temporal dynamics, predictive capability, and systematic validation, and they fail to exploit the rich, structured historical data captured through repeated risk assessments, mitigation updates, and review cycles (Quinn et al., 2024; Bonet et al., 2021).

Moreover, although machine learning techniques such as ensemble methods and boosting algorithms have demonstrated strong predictive performance in fraud detection and risk classification tasks, their application to internal fraud risk registers introduces significant unresolved model risk concerns. These include sensitivity to subjectively assessed inputs (e.g., probability and impact scores), instability under evolving operational and technological risk environments, and challenges related to interpretability and auditability for regulatory review (Bonet et al., 2021; Lazar, Qi and Tunaru, 2024). In regulated banking contexts, where models directly inform control prioritisation and compliance decisions, such limitations are non-trivial. Existing studies largely adopt a model-centric perspective, focusing on classification accuracy or loss prediction, while paying limited attention to deployment realities, governance structures, and the need for continuous monitoring and validation over time (Milojević and Redzepagic, 2021; Daramola, Chy and Fonkem, 2025). As a result, the integration of machine learning into enterprise internal fraud risk management remains fragmented and insufficiently aligned with regulatory expectations for model risk management.

This research addresses these gaps by focusing explicitly on internal fraud risk and by reconceptualising enterprise IT and operational risk registers as dynamic, predictive data sources rather than static governance artefacts. Using structured risk register data drawn from one or more systemically important banking institutions with comparable risk taxonomies, the study develops and evaluates a machine learning-based internal fraud risk scoring framework. *The proposed framework embeds mechanisms for model risk assessment, explainability, and continuous monitoring, ensuring robustness across evolving risk environments and alignment with regulatory, operational, and governance requirements in banking.*

### 3.0 Research Objectives

This study is structured around three focused and examinable objectives:

- a. To develop and empirically evaluate machine learning-based internal fraud risk scoring models using structured enterprise IT and operational risk register data from commercial banking institutions.
- b. To assess model risk in internal fraud detection by analysing the stability, sensitivity to inputs, and interpretability of supervised (XGBoost) and unsupervised (Isolation Forest) models across different risk environments.

- c. To examine how MLOps practices adopted within banking operations support *continuous internal fraud risk monitoring*, model governance, and regulatory compliance, and to assess their impact on model reliability and auditability.

## 4.0 Research Questions

- a. How effectively can machine learning models trained on Enterprise Risk Registers (ERR) data predict internal fraud risk compared to traditional Probability  $\times$  Impact scoring approaches?
- b. What model risk issues, such as instability, sensitivity to subjective inputs, and overfitting, arise when applying XGBoost and Isolation Forest models to internal fraud risk scoring?
- c. How can *MLOps-enabled continuous monitoring* improve the reliability, transparency, and governance of internal fraud risk models in regulated banking contexts?

## 5.0 Methodology and Data

### 5.1 Data Sources

The primary dataset will consist of enterprise IT and operational risk register data from one or more commercial banks. The dataset includes structured variables such as:

- Risk category (e.g. insider abuse, system misuse, control circumvention) (Quinn et al., 2024)
- Raw probability and impact assessments (Salo et al., 2022)
- Treated probability and impact assessments (Salo et al., 2022)
- Treatment status, mitigation maturity, and control costs
- Risk ownership, review dates, and audit annotations

These variables reflect how internal fraud risks are identified, assessed, mitigated, and reviewed in real banking environments. They provide suitable inputs for both supervised (e.g. XGBoost) and unsupervised (e.g. Isolation Forest) machine learning models, enabling comparative analysis across institutions and supporting rigorous model risk evaluation (Salo et al., 2022).

### 5.2 Model Development

The empirical analysis will focus on a *comparative modelling framework*:

- *XGBoost* for supervised internal fraud risk scoring, leveraging non-linear interactions and imbalanced data handling (Supriyadi, Priyarsono and Andati, 2023)
- *Isolation Forest* for unsupervised detection of emerging or previously unseen internal fraud patterns (Ski, 2024)
- *Baseline logistic or ordinal regression* models for benchmarking

Explainable AI techniques, particularly SHAP value, will be applied to ensure transparency and governance readiness of model outputs (Srivalli and Sumanthi, 2025).

### 5.3 Model Risk and Validation

Model performance and model risk will be evaluated using:

- Out-of-sample validation and rolling-window testing (Zhang et al., 2025)
- Stability analysis across successive risk review cycles (Al Janabi, 2024)
- Sensitivity analysis of probability, impact, and treatment-related inputs (Hossain, 2022)
- Explainability and auditability assessments aligned with regulatory expectations for model risk management (Srivalli and Sumanthi, 2025).

This structure explicitly separates risk measurement from risk governance, addressing a key gap in existing fraud modelling studies.

### 5.4 MLOps-Enabled Continuous Monitoring

Rather than designing a bespoke MLOps architecture, this research will examine how machine learning models for internal fraud risk are *operationalised, monitored, and governed within existing banking environments that have adopted MLOps practices*.

The study will draw on:

- Observed MLOps workflows within participating banks, including model deployment, monitoring, retraining, and version control practices
- Documentation and interviews with risk, IT, and compliance stakeholders (where feasible) to understand governance, auditability, and regulatory constraints
- Empirical analysis of model performance and stability before and after integration into continuous monitoring pipelines

Specific focus will be placed on:

- Data drift and concept drift monitoring
- Retraining triggers and validation cycles
- Integration of explainability tools into operational workflows
- Alignment with regulatory expectations for model risk management and auditability

This approach allows the research to evaluate how MLOps enhances continuous fraud risk monitoring in practice, without transforming the study into a systems engineering exercise, while remaining grounded in real-world banking constraints.

## 6.0 Expected Contributions

### Methodological contribution

This research will develop and empirically evaluate a *hybrid internal fraud risk scoring framework* that combines supervised (XGBoost) and unsupervised (Isolation Forest) machine learning methods using *Enterprise Risk Registers (ERR)* data. By moving beyond static Probability × Impact matrices, the study contributes a *dynamic, data-driven alternative* to internal fraud risk measurement grounded in real banking practice (Ski, 2024; Supriyadi, Priyarsono and Andati, 2023).

### Model Risk and Governance Contribution

The study will provide *systematic evidence on model risk* in ML-based internal fraud detection, examining stability across review cycles, sensitivity to subjective risk inputs, and interpretability under regulatory scrutiny. This extends the model risk literature into the underexplored domain of *enterprise risk register-based fraud modelling*, directly engaging with concerns highlighted in financial econometrics and model risk research (Lazar, Qi and Tunaru, 2024).

### Empirical Contribution

Using real-world risk register data from one or more *systemically important commercial banks*, the research will generate *empirical benchmarks* comparing traditional risk scoring approaches with ML-based methods for internal fraud detection. This provides rare, practice-grounded evidence in a domain where access to operational risk data is typically limited (Quinn et al., 2024).

### Practical and Regulatory Contribution

The research will deliver *actionable guidance* for banks on how internal fraud risk models can be deployed, monitored, and governed using MLOps principles. By examining continuous monitoring, retraining, explainability, and auditability, the study informs *regulatory-compliant deployment* of ML in fraud risk management, aligning with emerging expectations under Basel III/IV, GDPR, and AI governance frameworks (Daramola, Chy and Fonkem, 2025).

## 7.0 Fit with Supervision

This project aligns closely with *Professor Emese Lazar's expertise in risk measurement, model stability, and applied financial econometrics*, particularly her work on model risk and the robustness of risk models under uncertainty (Lazar and Xue, 2020; Lazar, Qi and Tunaru, 2024). While Professor Lazar's research has primarily focused on market and financial risk, this project extends those core methodological and governance concerns into the *internal fraud and operational risk domain*, using structured enterprise data and machine learning techniques.

The emphasis on *model risk assessment, stability analysis, and interpretability* ensures strong theoretical grounding, while the use of real banking risk register data and MLOps-enabled monitoring frameworks ensures practical relevance. My professional background in banking systems, enterprise risk governance, and large-scale data analytics positions me well to bridge econometric theory and real-world deployment challenges. I would greatly value the opportunity to further refine and develop this research under Professor Lazar's supervision.

## Reference

- Al Janabi, M.A., 2024. Unlocking the Microstructure of Liquidity Risk: Understanding Interactions with Other Financial Risks and Best Practices in Oversight and Governance. In *Liquidity Dynamics and Risk Modeling: Navigating Trading and Investment Portfolios Frontiers with Machine Learning Algorithms* (pp. 79-167). Cham: Springer Nature Switzerland.
- Beckley, J., 2025. Advanced risk assessment techniques: Merging data-driven analytics with expert insights to navigate uncertain decision-making processes. *Int J Res Publ Rev*, 6(3), pp.1454-1471.
- Bonet, I., Peña, A., Lochmuller, C., Patiño, H.A., Chiclana, F. and Gongora, M., 2021. Applying fuzzy scenarios for the measurement of operational risk. *Applied soft computing*, 112, p.107785.
- Daramola Olaniyi, A.K., Chy, A.M.R. and Fonkem, B., 2025. Integrated ML Feature Governance for Financial Risk Scoring: An MLOps and Compliance Framework, *Economics and Financial Policymaking*.
- Hossain, M.N., 2022. Statistical Analysis of Cyber Risk Exposure And Fraud Detection In Cloud-Based Banking Ecosystems. *ASRC Procedia: Global Perspectives in Science and Scholarship*, 2(1), pp.289-331.
- Ilori, O., Nwosu, N.T. and Naiho, H.N.N., 2024. Advanced data analytics in internal audits: A conceptual framework for comprehensive risk assessment and fraud detection. *Finance & Accounting Research Journal*, 6(6), pp.931-952.
- Lazar, E. and Xue, X., 2020. Forecasting risk measures using intraday data in a generalized autoregressive score framework. *International Journal of Forecasting*, 36(3), pp.1057-1072.
- Lazar, E., Qi, S. and Tunaru, R., 2024. Measures of model risk for continuous-time finance models. *Journal of Financial Econometrics*, 22(5), pp.1456-1481.
- Milojević, N. and Redzepagic, S., 2021. Prospects of artificial intelligence and machine learning application in banking risk management. *Journal of central banking theory and practice*, 10(3), pp.41-57.
- Oko-Odion, C. and Angela, O., 2025. Risk management frameworks for financial institutions in a rapidly changing economic landscape. *Int J Sci Res Arch*, 14(1), pp.1182-1204.
- Quinn, S., Quinn, S., Ivy, N., Barrett, M., Witte, G. and Gardner, R.K., 2024. Staging cybersecurity risks for enterprise risk management and governance oversight. *US Department of Commerce, National Institute of Standards and Technology*.
- Salo, A., Tosoni, E., Roponen, J. and Bunn, D.W., 2022. Using cross-impact analysis for probabilistic risk assessment. *Futures & foresight science*, 4(2), p.e2103.
- Ski, M.C., 2024. An overview of outlier detection methods. *London J. Eng. Res*, 24(2), pp.37-79.
- Srivalli, K.S. and Sumanthi, D., 2025. Enhancing Financial Risk Assessment through Explainable AI: A SHAP-Based Approach for Transparent Decision-Making. Available at SSRN 5190418.
- Supriyadi, H., Priyarsono, D.S. and Andati, T., 2023, May. Analysis of Internal Fraud in the Microloan Process with Confirmatory Factor Analysis (CFA) and the Extreme Gradient Boosting (XGBoost) Method. In *Business Innovation and Engineering Conference (BIEC 2022)* (pp. 238-255). Atlantis Press.
- Temuçin, T.S., 2025. ROLE OF MACHINE LEARNING IN INTERNAL FRAUD DETECTION. *TIDE Academia Research*, 6(2), pp.151-172.

*Zhang Parker, C., Jiang, L., Cho, S. and Vasarhelyi, M.A., 2025. Predicting Material Misstatements Using Machine Learning. The Accounting Review, 100(6), pp.225-262.*