TERMS OF REFERENCE: DEVELOPMENT OF A FRAUD MITIGATION STRATEGY/FRAMEWORK

BACKGROUND:

The Reserve Bank of Malawi aims to strengthen its financial ecosystem by implementing a comprehensive fraud mitigation strategy. The objective is to enhance the resilience of payment systems and protect financial transactions against fraud risks. With the rising fraud cases among retail payments in Malawi, this initiative is vital for safeguarding Malawi's financial infrastructure against fraud and improving the trust and reliability of its payment systems.

OBJECTIVES:

- Develop a comprehensive fraud mitigation strategy/framework
- Identify current and emerging fraud patterns within Malawi.
- Recommend measures to improve fraud detection, prevention, and response.
- Enhance the capabilities of financial institutions and other stakeholders in the digital financial services ecosystem in managing fraud risks through capacity building.
- Ensure alignment with international best practices and regulatory standards.
- Assess the vulnerabilities / weaknesses being exploited by fraudsters
- Analyse fraudster behavioural patterns and evolving methods used to commit fraud
- Identify emerging types and trends of fraud in the region, and at a global level and recommend prevention strategies
- Recommend strategies and a platform, using experiences from other regions within the world, on stakeholder collaboration on fraud

SCOPE OF WORK:

- Conduct a thorough analysis of the current fraud landscape in the financial sector and review existing policies, procedures, and controls related to fraud detection and prevention.
- Identify and assess the key fraud risks facing the retail payments financial ecosystem including examining financial records, transactions, and other relevant documentation to identify irregularities and historical patterns
- Develop a fraud mitigation strategy/framework that includes:
    - Fraud risk management principles and guidelines.
    - Preventive measures, including customer education and system controls.
    - Detection mechanisms for early identification of fraud incidents.
    - Incident response protocols and recovery measures.
    - A monitoring and evaluation framework to assess the strategy's effectiveness.
- Conduct training and information sessions for relevant stakeholders to strengthen fraud management skills and awareness.

- Conduct group or individual interviews with key personnel from different departments and at all levels of the organization to gather insights into potential vulnerabilities and obtain a broader perspective on organizational culture and understanding of fraud mitigation.
- This review aims to assess the switch's operational efficiency, compliance with best practices, and ability to support the country's digital financial services landscape. The review will also aim to identify any gaps that could potentially be exploited for fraud.
- Development of a Technical Specification/Business Requirements Document that can be used to identify a tool for managing fraud.
- Analyze current fraud detection systems, policies, procedures, and controls and benchmark against industry standards ensuring compliance to domestic and international laws then outline strengths, weaknesses, and areas needing enhancement.
- Review historical data on fraud and draft a matrix on fraud threats and using analytical tools, categorise fraud based on type and highlight the high, medium and low fraud threats
- Evaluate system's resilience and alignment with best practices and international standards on fraud
- Design a comprehensive fraud prevention framework to prevent, detect, and respond to fraud and align the framework with international standards and best practices
- Assess the entire payment ecosystem and supporting infrastructures and then draft clear anti-fraud policies with defined roles and responsibilities
- Review and assess the KYC and AML policies and procedures to identify weaknesses and gaps. Recommend areas that need strengthening
- Conduct structured sessions with different stakeholders including consumers to understand the different perspectives of fraud
- Explore different methods and datasets that can be used to detect and prevent fraud
- Analyze ways on how AI, blockchain and ML can be deployed to support fraud prevention strategies
- Design frameworks that will strengthen operational efficiency and reduce fraud risk in Malawi
- Design an implementation plan for the fraud mitigation strategy to guide the bank on how to implement and enforce the strategy.

DELIVERABLES:

- Inception report outlining the work plan and methodology.
- Situation analysis report on existing fraud risks and mitigation measures.
- Draft fraud mitigation strategy/framework for review.
- Final fraud mitigation strategy/framework incorporating stakeholder feedback. This should include an implementation plan for rolling out the strategy.

DURATION AND TIMELINE:

The assignment is expected to be completed within 3-4 months, with the following key milestones:

- Inception report: End of Month 1
- Situation analysis report: End of Month 2
- Draft framework: End of Month 3
- Final framework and training: End of Month 4

QUALIFICATIONS AND EXPERIENCE:

- Minimum 10 years of experience in financial fraud management, cybersecurity, or payment system security.
- Expertise in developing fraud risk management frameworks for financial institutions.
- Familiarity with international standards on fraud risk management (e.g., ISO 31000/37003).
- Strong analytical, writing, and stakeholder engagement skills.

REPORTING AND SUPERVISION:

The consultant/firm will report to the Director of Payment Systems at the Reserve Bank of Malawi and will work closely with a designated project management team.

The consultant will also report to the Regional Director, East & Southern Africa at AfricaNenda.

Submissions

Technical and Financial Proposals should be submitted electronically to info@africanenda.org before 24th December 2024, and the subject line should read "Development of a Fraud Mitigation Strategy/Framework", and relevant files labelled accordingly. Please note that incomplete or late applications will not be considered.