AML/CFT/CPF TRAINING FOR MLCOs OF INSURANCE COMPANIES AND INSURANCE BROKERS

Presenters:
Mr. BENJAMIN WESONGA

Ms. NABAGGALA PHIONAH:

Financial Intelligence Authority
Safe money for a Secure Market

AGENDA

Financial Intelligence Authority
Safe money for a Secure Market

- Role of MLCOs Officer
- ML/TF Risk assessment for insurance sector(RBA Approach)
- Emerging Technologies in AML/CFT
- Sanctions Regime

Role of MLCOs

1. Implement AML and KYC procedures approved by the board and management to ensure regulatory compliance on a day-to-day and long-term basis
2. Training and awareness, ensure employees and new staff are properly trained, have access to AML and KYC policies, and are equipped with appropriate tools to handle ML, and Suspicious Transactions.

3. Have adequate internal control systems to prevent and detect suspicious transactions and money laundering activities.

Role of MLCOs

5 . Conduct regular risk assessments to identify potential money laundering risks and implement measures to mitigate them, evaluate the effectiveness of existing controls, and recommend improvements.

6. MLCO acts as a liaison officer between financial FIA and the insurance company, they respond to regulatory inquiries, audits, and inspections related to AML compliance

7. Internal Audits, oversee internal audits to ensure the effectiveness of the AML program, review transactions monitoring system

RBA

- FATF emphasizes increased emphasis on the RBA to AML/CFT, especially in relation to preventive measures and supervision, countries are required to apply preventive measures that are commensurate to the nature of risks to focus their efforts in the most effective way.
- Poor risk assessment can lead to box ticking application and most importantly does not reflect the real ML/TF risk threats of institutions
- There is inability to identify , assess and mitigate ML/TF risks, including the fundamental elements of customer identification and verification

RBA

- The application of RBA is therefore not an optional, but a prerequisite for the effective implementation of the FATF standards

It involves

- Identifying ML/TF risks
- Assessing ML/TF risk
- Mitigating ML/TF risk

RBA

There are different categories of risks

- Product risks
- Distribution risk
- Geographical risks
- Customer risks

National Risk Assessment

Findings

Sectors	Risk Score
Banks	High
Securities	Medium
Insurance	Medium
Real Estate	High
Casinos	High
Lawyers	High
Accountants, Auditors, Tax Advisors	Medium-Low
Dealers in Precious Metals & Stones (DPMS)	High
Money Value Transfer Services (MVTS)	High
Forex Bureaus	Medium

Continued....

RBA-customer

- Customers and related parties(policy holder and if any, its beneficial owner
- Customer growth-rapid growth or turnover of customer base in terms of amount and customer diversity pose higher ML/TF risks
- Individuals who are more difficult to identify and with the involvement of parties
- Higher-risk individuals. Customers previously reported by the insurer or intermediary to FIA or who operate in a high-risk industry or profession from an AML/CFT perspective
- Structures that make it difficult to identify the beneficial owner of the policyholder or the beneficiary
- Complex ownership and control structures involving multiple layers of shares registered in the names of legal entities

Customer Based Risk Attributes used to assess ML/TF Vulnerabilities to

ATTRIBUTE	LOWER RISK	HIGHER RISK
Identification	Customer provide photo identification or can be identified using third party sources	Customer has difficult producing identification or th authenticity of identificatio provided is questionable
Third party relationship	No third party involvement	- Controlled by a third o multiple indicators of thir party deposits or payments - Controlled by a gatekeepe without any interaction wit the beneficial owner
Customer legal form	- Customer is a living person - Customer is a large, publicly traded legal entity with clear ownership and control	- Customer is a legal entit with a complex structur difficult to ascertain thos who own or control th entity Policy holder and th

RBA-customer

- **Payment methods**
- **Payment methods that may contribute to increased ML/TF risks e.g. cash, payment from different bank accounts without explanation, the payment received from unrelated third parties**
- **Origin or source of funds and wealth**
- **Unclear of suspicious sources of wealth or sources of funds that are involved in the business relationship**

RBA-customer

- **Products and services**
- associated with high-risk payments, products that may favor international customers, cash, third parties, and complex payments
- Products that accumulate large funds, transact large sums or allow high amounts of withdraws
- Products that favor anonymity or are easily transferable

XAMPLE OF PRODUCT ESCRIPTION	TYPICAL FEATURES	INDICATIVE RISK RATING
.Complex products with otential multiple investment ccounts and or products ith returns linked to the erformance of an underlying nancial asset xample of products Universal life Assurance schemes Investment linked Unit linked	• Offers the ability to hold funds and assets • May offer the option of asset transfers into the policy • May offer the option of asset transfers into the policy • Full or partial underlying investments under control of the customer • May have a high limit of funds held	Higher risk compared to other products
.Products designed for high et worth persons or for ndividuals generally with uaranteed returns. xample of product Individual life insurance Traditional whole life	• Offers the ability to hold funds • Only with high limit for funds held • Underlying investments managed by the insurer	High/Moderately high risk compared with other life insurance products
.Product that pays a periodic ncome benefit for the life of person	• May have a high limit for funds held • Offers the ability to hold	Moderate risk compared with other life insurance

RBA-customer

- **Distribution channels**
- Channels that do not provide for a physical meeting between the customer and an employee and are not supported by mitigation measures
- Reliance and outsourcing to third parties that are not subjected to the same AML/CFT obligations as insurance companies
- **Geography**
- Products and services that are marketed or sold in higher ML/TF risk countries
- Customers, beneficiaries, policyholders, and parties that are linked to high ML/TF risk countries

International and domestic geographical risk factors

ATTRIBUTE	LOWER RISK	HIGHER RISK
Higher crime regions	Customer does not reside in a region with higher frequency and severity of crimes	The customer resides in a region with high frequency and severity of crimes with money laundering and terrorism financing
History of high risk activity or fraud	Customer does not reside in a region that experiences a higher incidences of high risk activity or fraud	Customer resides in a region that experiences a higher incidence of high risk activity or fraud
Foreign tax or physical residency of customer	Countries ranked as low by the life insurer	Countries risk ranked as high by the insurer
Foreign ties transactions	Customer does not have any indicators of foreign residency or transactions	Customer has requested or performed transactions with ties to high risk countries

Risk mitigation controls

After assessing the ML/TF risks, insurance companies should develop and implement mitigating controls proportionate to ML and TF risks identified and to the complexity, nature, and size of the entity resources to mitigate their most significant

- **Customer Due Diligence(CDD)**
- **Simplified Due Diligence(products that only pay out at death, customers that are publicly listed companies on recognized exchange**
- **Enhanced Due Diligence(where third party payer is not the account holder**

Risk mitigation controls

- **Ongoing Risk Monitoring and Mitigation**
  - **It involves the scrutiny of activity to determine whether they are consistent with the information held on the customer and the nature and purpose of the business relationship**
- **Reporting Suspicious Transactions**
  - **If the insurance company suspects have reasonable grounds to suspect that funds are the proceeds of criminal activity or related to terrorist financing**
- **Internal controls(assessment controls and Governance**

ML/TF RED FLAGS

Financial Intelligence Authority
Safe money for a Secure Market

1. **Large single premium payment that is inconsistent with financial profile**

2. **Clients canceling policies early and requesting refunds most times to be paid to third parties in a different currency**

3. **Multiple small policies to avoid detection**

4. **Reluctancy to provide information and providing information that cannot be verified**

5. **Using third parties to manage their insurance policies**

ML/TF RED FLAGS

6. **Suspicious insurance products.**

7. High-risk jurisdictions, transactions involving clients or beneficiaries from countries with a lack of regulatory oversight, or jurisdictions known for weak AML/CFT controls.

8. Transaction irregularities, inconsistent payment sources

9. Insurance funds are directed to NPOs suspected of being used by terrorists.

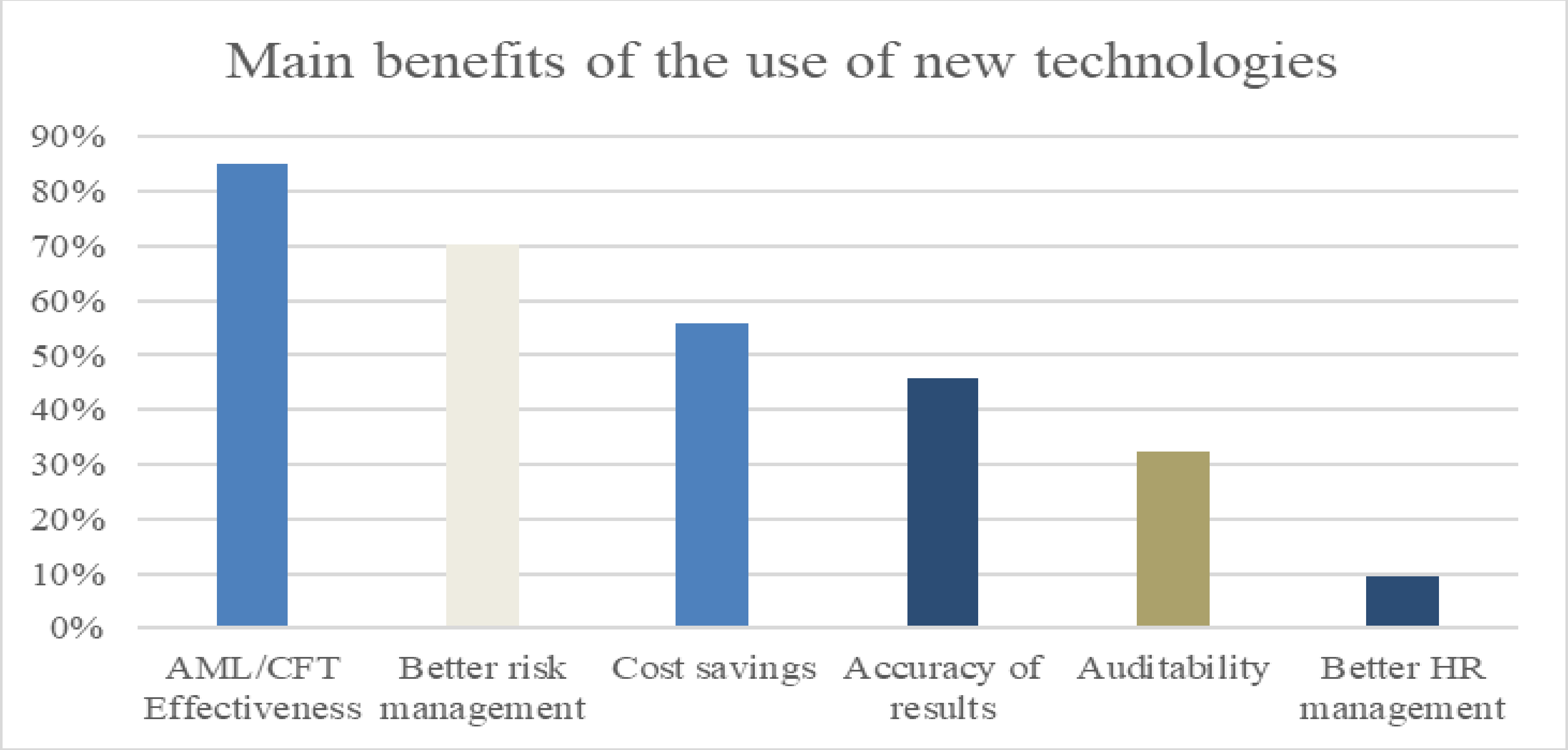
10. Transactions involving individuals or organizations that are on international sanctions lists.

ML/TF RED FLAGS

Insurance companies need to implement robust AML/CFT compliance programs to detect and prevent red flags, these include

- **Thorough customer due diligence(CDD)**
- **Transaction monitoring**
- **Continuous reporting of suspicious activities**
- **Continuous training of employees on AML/CFT/PF matters**
- **etc.**

Benefits of new technology



Benefits of the use of new technology

- Strengthen identification and Verification of customers: Can enable non face to face verifications In the context of remote onboarding and authentication AI, including biometrics, machine learning and liveness detection techniques can be used to perform: micro expression analysis, anti-spoofing checks, fake image detection, and human face attributes analysis.
- Monitoring of the business relationship and behavioral and transactional analysis:
- Supervised machine learning algorithms: Allow for a quicker and real time analysis of data according to the relevant AML/CFT requirements in place.
- Alert Scoring: Alert scoring helps to focus on a patterns of activity and issue notifications or need for enhanced due diligence.

When can machine learning be used

Identification and implementation of regulatory updates:

Machine Learning techniques

- can scan and interpret big volumes of unstructured regulatory data sources on an ongoing basis to automatically identify, analyze and then shortlist applicable requirements for the institution;

Fore example data on large cash to predict the transactions in the future. To determine the most probable outcome. Garbage in garbage out, if given good quality data it gives good results and the reverse is true.

Note AI has to be human monitored at the tail end to verify the decisions made.

Benefits of the use of new technology for AML/CFT

- Distributed Ledger Technology
- DLT may improve traceability of transactions on a cross border basis, and even global scale, potentially making identity verification easier. A responsible and regulated use of DLT for data and process management purposes may also speed up the CDD process, as consumers can authenticate themselves and can even be automatically approved or denied through smart contracts that verify the data

Benefits of the use of new technology for AML/CFT

Financial Intelligence Authority
Safe money for a Secure Market

- under appropriate safeguards and regulatory environment, transactions can potentially be managed via a single ledger shared among several institutions across jurisdictions, or via interoperable ledgers. This would significantly increase the monitoring possibilities compared to the existing frameworks.

- DLT technologies may also offer benefits for managing CDD requirements contributing to user concerns regarding this process, greater cost effectiveness for the private sector, and a more accurate and quality-based data pool. For example, in China, DLT is being used by financial institutions to share watch lists or red flags on the basis the scope of confidentiality permitted by this system.

When can machine learning be used

- **Despite its merits, DLT seem to continue to pose challenges and raise significant concern from an AML/CFT perspective, as seen in the regulation and /supervision of virtual assets. Transactions through conventional intermediaries such as banks, transactions in virtual assets (VA) based on DLT are decentralized in nature and enable un-intermediated peer to peer transactions to take place without any scrutiny.**

Benefits of the use of new technology in AML/CFT

- Digital ID provides one of the best case studies for this area, as it has been widely adopted and supported in many jurisdictions (and FATF has issued guidance on its use). Evidence suggests that the COVID-19 crisis has further promoted demand for remote financial services delivery. In fact, eID and verification is among the "most mature and instantly useful elements of technology in AML". (Richard Grint et al, 2017[14]) It is also among the most recognizable and often mentioned by respondents to the questionnaire as a good practice in AML/CFT .

Benefits of the use of new technology

- Digital ID may improve, for example, customer access to financial services through mobile devices and smart phones whilst ensuring the security and accuracy of customer information through biometric information as a supplement to personal identity information. Some financial institutions may, based on basic ID information, increase the diversity of data sources by collecting additional data from customers, with their permission, which ultimately strengthens the knowledge and ability to manage the business relationship.

Use of new technology for CDD

- Additionally, onboarding tools that allow for quick CDD and client traits analysis (such as anti-fraud software and others would also enrich the CDD and monitoring process and lead to a more accurate understanding of the nature of the business relationship, as well as its impact to the institutions.

- The enhanced use of technologies, for client screening and matching, holds great potential to improve the compliance processes, as reliance on out of date and regionally irrelevant sanctions', PEP and other lists are acknowledged as an area in need of improvements.

- Such tools allow differentiation of similar names and other elements of identification, overcome language differences, identify cross-references with adverse media information and different databases.

Use of new technology for CDD

- **Natural language processing and more advanced fuzzy matching tools could offer significant advantages to this function. Data harmonization would also help to eliminate false positives and fraud attempts, as actors would begin relying on pooled information and varied verification systems.**

Use of APIS- New technology

- Type of software which allows different applications to connect and communicate.

- APIs among the most used and relevant solutions to the identified money laundering and terrorist financing problems.
- Their utility for AML/CFT lies in the ability to, for example, connect customer identification software with monitoring tools, or risk and threats identification tools with customer risk profiles in order to generate alerts or alter risk classifications as relevant. APIs allow this integration to happen much more quickly and with much larger datasets. This is particularly relevant as one of the most difficult challenges for many financial institutions is the integration of many different and often incompatible systems, including legacy technologies and specialized tools, created by different developers.

AAPIs

- **API's also offer great value to the public sector by helping them access business registries and others.**

APIs

- The use of APIs enables the relevant authorities to obtain real-time data on the volume of importation of foreign currencies and all banking operations related to foreign currencies.

APIs

The use of APIs by supervisors, when combined with AI-driven analytics, could increase the efficiency of mandated reporting practices and the quality of the risk-based supervision.

This type of tool allows supervisors to process historical data with onsite inspections data and contextual factors and generate automated reports for consideration and defining action.

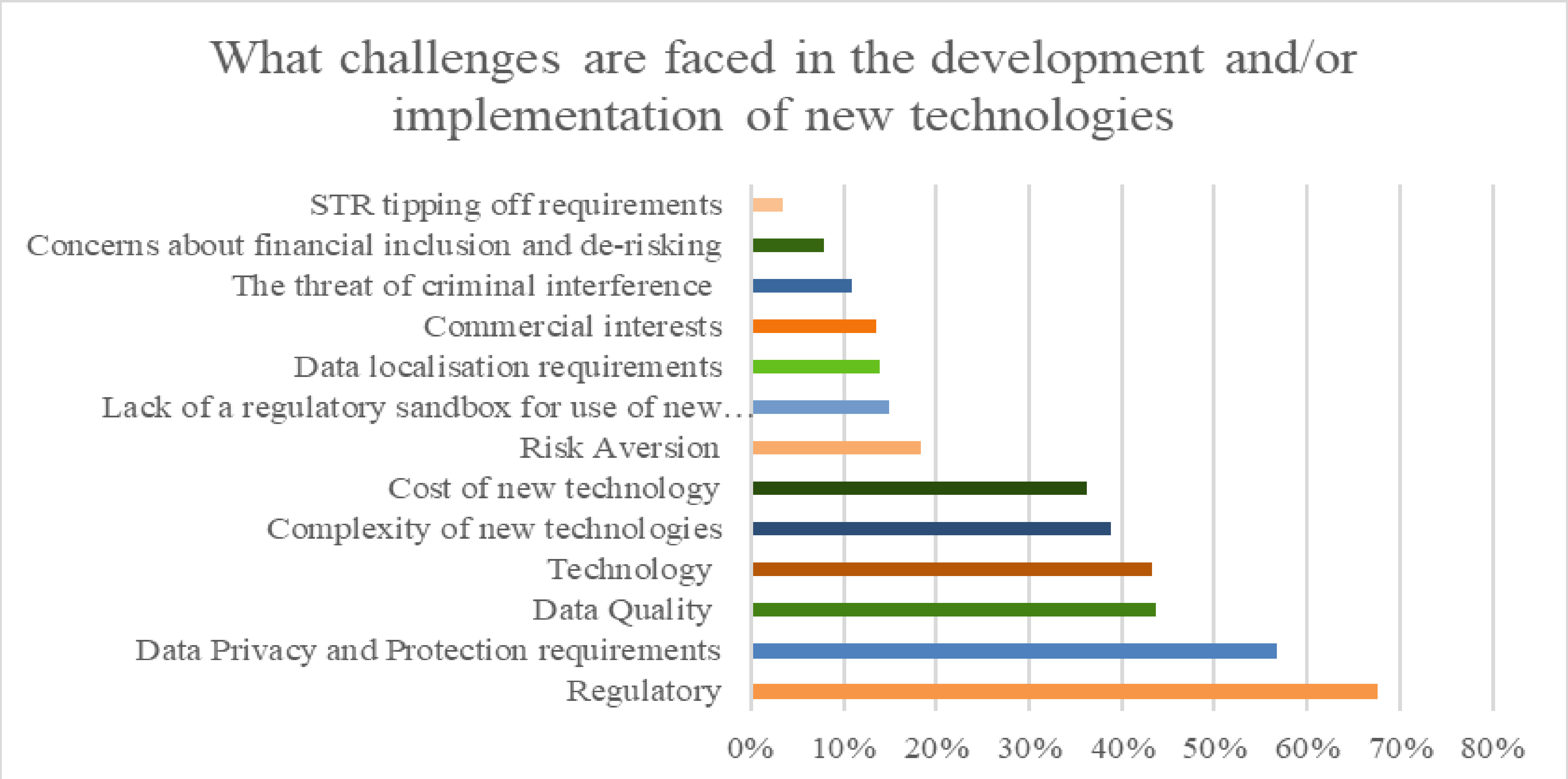
Benefits of new technologies

PEP-screening solution

Screening of PEPs and their relationships is a resource-heavy manual process for obliged entities and requires them to obtain personal data about their customers. such relationships could to a large extend be mapped through public registers,.

The analysis looks into establishing a public PEP-screening solution which could improve the quality and reduce the cost of PEP-screening through increased digitization, while at the same time minimizing the collection of personal information.

Challenges of new technology



What challenges are faced in the development and/or implementation of new technologies

Challenges of new technologies

Standardization of data

The use of new technologies for AML/CFT can only truly become effective if systems are based on standardized data that is easier for technology developers to integrate into their tools, easy to understand and explain to non-experts, and easy to communicate to counterparts and competent authorities when needed.

Cont'd

Reliable feed back by FIUs

This issue also shows the importance of public authorities, particularly FIUs, providing reliable feedback to reporting entities on suspicious activity and ML cases that can be used for training purposes.

Cont’d

Financial Intelligence Authority
Safe money for a Secure Market

Reliable feed back from FIUs and competent authorities can support Fis to train and inform internal compliance teams and systems.

challenges

Data harmonization (or lack thereof) was also mentioned as an additional obstacle,

- **It is costly investing in new technologies and expertise**
- **fine-tuning and adjustment to different jurisdictional requirements and formats.**

Data harmonization therefore offers significant advantages

- **it allows actors to converge in goals, for example, a common transaction monitoring, providing feedback to private sector and risk assessments.**

Challenges

Interpretability of data by users

The real or perceived issues of interpretability have also led to constraints in the ability to build trustworthy relationships between technology providers and users, and a lack of trust that data processed through new technologies can be robust.

Challenges- transparency and accountability

Technology that does not permit accountability, transparency and the supervision of entities using new technologies.(complexity)

Supervisory Authorities should reflect on the scrutiny required for example as service providers to regulated entities or via separate regulation and supervision

Technology that cannot permit expanded access for regulated entities to government data bases.

WAY FORWARD

Desire to have "technology-active supervisors" –

- **supervisors willing to engage with technology developers –To understand the new technology and innovations**

Conclusion

- Increased uptake of new technologies will enhance the supervisory practices, a balance must be struck between the importance of integrating technologies and

Sanctions Regime

Administrative Sanctions

Section 23(q) of the AMLA Cap 118 and regulation 54(e) of the AMLA regulations as amended, give powers to FIA to impose administrative sanctions for non-compliance with directives, guidelines, or requests issued by FIA. These include recommendations for the dismissal of the entire Board, and management team and issuance of warning letters among others.

Regulation 53 of the AML Amendment Regulations gives powers to supervisory Authorities to impose sanctions for non compliance.

Pecuniary Sanctions/Fines

Breach	Regulation	Maximum currency point	Amount (Ugx)
Failure to provide continuous training of employees, managers and director (natural person)	R.11(6)(b)	500	10,000,000
Failure to carryout due diligence (corporate person)	R.17A(a)	25,000	500,000,000
Failure to carryout due diligence (natural person)	R.17A(b)	5,000	100,000,000
Penalty for contravention of regulations 18, 19, 20, 21,22, 23, 24, 25, 26 and 27 (Corporate person)	R.27A(a)	25,000	500,000,000
Penalty for contravention of regulations 18, 19, 20, 21,22, 23, 24, 25, 26 and 27 (natural person)	R.27A(b)	5,000	100,000,000
Failure to keep records (corporate person)	R.28(7)(a)	3,750	75,000,000
Failure to keep records (natural person)	R.28(7)(b)	3,750	75,000,000
Failure to implement appropriate risk management systems to determine whether a person or customer is a PEP (corporate person)	R.29(5)(a)	12,500	250,000,000
Failure to implement appropriate risk management systems to determine whether a person or customer is a PEP (natural person)	R.29(5)(b)	5,000	100,000,000
Failure to ensure that its foreign branch or subsidiary apply due diligence measures and other measures relating AML/CFT (corporate person)	R.30(5)(a)	12,500	250,000,000

Continued....

Pecuniary Sanctions/Fines

	Regulation	Maximum Currency Point	Amount (Ugx)
Failure to ensure that its foreign branch or subsidiary apply due diligence measures and other measures relating AML/CFT (natural person)	R.30(5)(b)	5,000	100,000,000
Failure to undertake the measures before establishing correspondent financial business relationship (corporate person)	R.31(4)(a)	12,500	250,000,000
Failure to undertake the measures before establishing correspondent financial business relationship (natural person)	R.31(4)(b)	5,000	100,000,000
Failure to develop and update on a regular basis a written risk-based customer acceptance policy for ongoing business relationships or single transactions (corporate person)	R.32(4)(a)	6,250	125,000,000
Failure to develop and update on a regular basis a written risk-based customer acceptance policy for ongoing business relationships or single transactions (natural person)	R.32(4)(b)	1,250	25,000,000
Penalty for breach of regulations 33, 34, 35, 36 and 37 (corporate person)	R.37A(2)(a)	12,500	250,000,000
Penalty for breach of regulations 33, 34, 35, 36 and 37 (natural person)	R.37A(2)(b)	250	5,000,000
Failure to establish the legitimacy of the source of funds and transactions involving a person or customer (corporate person)	R.38(4)(a)	6,250	125,000,000

Continued....

Pecuniary Sanctions/Fines

Breach	Regulation	Maximum currency point	Amount (Ugx)
Failure to establish the legitimacy of the source of funds and transactions involving a person or customer (natural person)	R.38(4)(b)	250	5,000,000
Failure to report suspicious activities and certain cash transactions (corporate person)	R.39(5)(a)	37,500	750,000,000
Failure to report suspicious activities and certain cash transactions (natural person)	R.39(5)(b)	12,500	250,000,000
Failure by the supervisory authority to report suspicious activities	R.40(3)	25,000	500,000,000
Failure to maintain records for a minimum of 10 years (corporate person)	R.42(9)(a)	2,500	50,000,000
Failure to maintain records for a minimum of 10 years (natural person)	R.42(9)(b)	5,000	100,000,000
Failure to carry out periodic independent audits to assess its compliance with the requirements of the Act and Regulations (corporate person)	R.43(3)(a)	6,250	125,000,000
Failure to carry out periodic independent audits to assess its compliance with the requirements of the Act and Regulations (natural person)	R.43(3)(b)	1,250	25,000,000
Failure to apply measures in respect of a person or customer from, or transactions involving, high risk countries (corporate person)	R.44(4)(a)	5,000	100,000,000
Failure to apply measures in respect of a person or customer from, or transactions involving, high risk countries (natural person)	R.44(4)(b)	500	10,000,000

Financial Intelligence
Authority
Safe money for a Secure Market

QUESTIONS?

Thank You!