OVERVIEW OF AML/CFT INTERNATIONAL STANDARDS

Presented to:

Insurance Regulatory Authority

-Stakeholders' Workshop

March 2019

Outline of Presentation

1. The AML/CFT Standards.
2. The Obligations of Financial Institutions
3. Risk Based Approach.

The Standard Setters

- Financial Action Task Force
- Sector-specific Groups:
  - Basel Committee on Banking Supervision
  - International Association of Insurance Supervisors (IAIS)
  - International Organization of Securities Commissions (IOSCO)
- United Nations
- AU, COMESA and EAC Protocols against ML/TF, Terrorism and Corruption

The Standard Setters

International Association of Insurance Supervisors (IAIS)

ICP 22 -Anti-Money Laundering and Combating the Financing of Terrorism

- The supervisor requires insurers and intermediaries to take effective measures to combat money laundering and the financing of terrorism.
- In addition, the supervisor takes effective measures to combat money laundering and the financing of terrorism.

Financial Action Task Force (FATF)

- The FATF is an inter-governmental body established in 1989 during the G7 Summit.
- Mandate is to set standards and to promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and the financing of proliferation, and other related threats to the integrity of the international financial system.

FATF Membership

- 37 member countries, GCC & EC. Plus 2 observer countries
- 9 FATF styled regional bodies (FSRBs) including ESAAMLG.
- 22 Observer Organizations including the AfDB, World Bank and IMF.

FATF R40: Why Are They Unique?

- Self & Mutual evaluations.
- Suspicious Transaction Reporting.
- Cooperation with FATF style regional bodies (FSRB). Total reach > 180 jurisdictions.
- Partnership with the World Bank and IMF on the Methodology For Assessing Compliance with Anti-Money Laundering And Combating The Financing of Terrorism Standards.
- Typologies exercises.
- ICRG exercise (formerly NCCT).

The Financial Action Task Force
WWW.FATF-GAFI.ORG
Summary of Recommendations

- Measures adapted to countries particular circumstances.
- Essential measures that countries should have in place to:
  - Recs 1- 2: identify the risks, and develop policies and domestic coordination;
  - Recs 3-8: pursue money laundering, terrorist financing and the financing of proliferation;
  - Recs 9-23: apply preventive measures for the financial sector and other designated sectors;

The Financial Action Task Force WWW.FATF-GAFI.ORG

Summary of Recommendations cont.:

- Recs 24- 25: enhance the transparency and availability of beneficial ownership; information of legal persons and arrangements;
- Recs 26-34: establish powers and responsibilities for the competent authorities (e.g., investigative, law enforcement and supervisory authorities) and other institutional measures; and
- Recs 35-40: facilitate international Cooperation (mutual legal assistance and extradition, and other forms of cooperation).

FATF Standards: Scope of Application

- Financial Institutions includes:
  - Banks
  - Securities firms
  - Insurance companies
  - Forex bureaus
  - Remitters

- FATF provides a definition for financial institutions that focuses on the nature of the business rather than what it is called.

Glossary – "Designated non-financial businesses and professions" means:

- Casinos (which also includes internet casinos)
- Real estate agents
- Dealers in precious metals
- Dealers in precious stones
- Accountants
- Lawyers & independent legal professionals
- Notaries
- Trust and Company Service Providers

Financial Institutions Responsibilities

1. Identify, assess, and adequately mitigant their ML/TF risks
2. Customer due diligence
3. Record keeping for five years minimum after termination of relationship
4. Transaction Monitoring and Reporting Suspicious Transactions (STRs)
5. Adequate internal control systems- including
   - Appointment of a money laundering reporting officer
   - Independent check
   - Training of staff and agents

The Obligations of Financial Institutions

Preventive Measures

Recommendation	Subject
Recommendation 9	Secrecy
Recommendation 10	Customer Due Diligence
Recommendation 11	Record Keeping
Recommendation 12	Politically Exposed Persons
Recommendation 13	Correspondent banking
Recommendation 14	Money or Value Transfer Services
Recommendation 15	New Technologies
Recommendation 16	Wire Transfers
Recommendation 17	Reliance on third parties
Recommendation 18	Internal controls and foreign branches and subsidiaries
Recommendation 19	Higher risk countries
Recommendation 20	Reporting of suspicious transactions
Recommendation 21	Tipping-off and confidentiality

R. 10 – Customer Due Diligence (CDD)

- Financial institutions (FIs) should be prohibited from keeping anonymous accounts or accounts in obviously fictitious names.
- When is it required?
  a) establishing business relations;
  b) carrying out occasional transactions above a threshold (EUR/USD15,000) or that are wire transfers:
  c) there is a suspicion of money laundering or terrorist financing; or
  d) the FI has doubts about the veracity or adequacy of previously obtained customer identification data.

R. 10 – CDD Measures

What is required

a) Identifying the customer and verifying the customers' identity using reliable, independent source documents, data or information.

b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner such that the financial institution is satisfied that it knows who the beneficial owner is.

- For legal persons and arrangements, understanding the ownership and control structure of the customer.

c) Understanding and obtaining information on the purpose and intended nature of the business relationship.

d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions

R. 10 – CDD

- All CDD measures under (a) to (d) above are to be implemented, but FIs should determine the extent of such measures using a Risk-Based Approach (RBA)
- Verification of Identity of the customer and the beneficial owner to be undertaken before or during the course of establishing a business relationship or conducting transactions for occasional customers.
- FIs may complete the verification as soon as reasonably practicable after the establishment of the relationship where ML and TF risks are effectively managed and where this is essential not to interrupt the normal conduct of business.

R. 10 – CDD

- Where the FI is unable to comply with the applicable requirements under paragraphs (a) to (d) above, it:
  - Should not open the account, commence business relations or perform the transaction;
  - Should be required to terminate the business relationship; and
  - Should consider making a suspicious transactions report in relation to the customer.
- The requirements are applicable to all new customers and to existing customers on the basis of materiality and risk.

CDD for beneficiaries of life insurance policies

- For life or other investment-related insurance business, FIs should in addition to the CDD measures required for the customer and beneficial owner, conduct the following CDD measures on the beneficiary(ies) of the life insurance and other investment related insurance policies, as soon as the beneficiary(ies) are identified/designated:
  a. For beneficiary(ies) that are identified as specifically named natural or legal persons or legal arrangements – taking the name of the person
  b. For beneficiary(ies) that are designated by characteristics or class or by other means – obtaining sufficient information concerning the beneficiary to satisfy the FI that it will be able to establish the identity of the beneficiary at the time of payout
- For both cases referred to in (a) and (b) above, the verification of the identity of the beneficiary(ies) should occur at the time of the payout.

CDD for beneficiaries of life insurance policies

- The beneficiary of a life insurance policy/investment-related product should be included as a risk factor by the FI in determining whether enhanced CDD measures should be applied.
  - If it is determined that a beneficiary who is a legal person or arrangement presents as a higher risk then the enhanced CDD measures should include reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary at the time of payout.
- If a FI is unable to identify the beneficiary it should consider making a suspicious transaction report.
- FIs should take reasonable measures to determine whether the beneficiaries and/or the beneficial owner of the beneficiary are PEPs. This should occur, at the latest, at the time of payout. Where higher risks are identified (e.g. a PEP) FIs should inform senior management before the payout is made, conduct enhanced scrutiny of the whole business relationship with the policy holder, and consider making a suspicious transaction report.

R. 10 – IN – CDD

- Enhanced CDD measures:
  - FIs should examine the background and purpose of all complex, unusual large transactions and all unusual patterns of transactions with no apparent economic lawful purpose
  - High Risk-Enhanced CDD measures-Increase the degree and nature of monitoring of the business relationship
- Simplified CDD measures:
  - Low Risks-FIs allowed to conduct simplified CDD measures
    - Not applicable: (i) if there is a suspicions of ML/TF, (ii) where specific higher-risk scenarios apply.
- Ongoing Due Diligence:
  - Documents/Data/Information collected under the CDD process/kept-up-to-date, particularly for higher-risk categories of customers.

R.11 – Record keeping

- FIs should be required to maintain all necessary records on transactions (domestic and international) to enable them to comply swiftly with information requests from competent authorities.

- FIs should keep all records obtained through CDD measures…including the results of any analysis undertaken for at least five years after the business relationship has ended or after the date of the occasional transaction.

- Records on transactions should be maintained for 5 years and must be sufficient to permit reconstruction of individual transactions so as to provide, if necessary evidence for prosecution of criminal activity.

Politically exposed persons (PEP's)- (R12)

- Domestic, Foreign and International PEP.
- Persons who hold or have held prominent public functions e.g. head of state or government, senior politicians, senior government, judicial or military officials, senior executives of state corporations, important political party officials.
- persons who hold or have held a prominent function at an international organization directors, deputy director, members of the board etc.
- Close relatives and associates included in definition

Requirements for Managing the Risk re PEPS

- Foreign PEPs (whether as customer or beneficial owner), in addition to performing normal CDD:
  - Have appropriate risk management systems to determine whether the customer or the beneficial owner is a politically exposed person (PEP).
  - Obtain senior management approval for establishing (or continuing, for existing customers) such business relationships.
  - take reasonable measures to establish the source of wealth and source of funds; and
  - conduct enhanced ongoing monitoring of the business relationship.

R. 15 - New Technologies

- Financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to:
  a) (a) the development of new products and new business practices, including new delivery mechanisms, and
  b) (b) the use of new or developing technologies for both new and pre-existing products.

- Ideally, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. The risk assessment should consider the development of appropriate measures to manage and mitigate those risks identified.

R.17 Reliance on Third Parties

- R.17 provides for countries to permit FIs to rely on third parties to perform elements of the CDD measures set out in R.10 provided certain criteria are met:
- Criteria that should be met are:
  a) The FI relying on a 3rd party should immediately obtain the necessary information concerning elements (a)-(c) of R.10.
  b) FIs should take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to CDD are available upon request without delay.
  c) The FI should satisfy itself that the 3rd party is regulated, supervised or monitored for, and has measures in place for compliance with, R.10 and R.11.
  d) When determining in which countries the 3rd party that meets the conditions above can be based, countries should have regard to information on the level of country risk.

Internal controls and foreign branches and subsidiaries

- **The AML/CFT program must include**:
  - Internal policies, procedures and controls
  - Training program for employees
  - Internal audit program
  - Screening procedures when hiring employees
  - Designation of a compliance officer at management level

R. 20 – Suspicious Transaction Reporting

- If a FI suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should report promptly its suspicions to the FIU.
  - "Criminal activity" refers to all criminal acts which would constitute a predicate offence for money laundering.
  - "Terrorist financing" refers to the financing of terrorist acts and also terrorist organizations or individual terrorists, even in the absence of a link to a specific terrorist act of acts.
  - All suspicious transactions, including attempted transactions, should be reported regardless of the amount.

Risk Based Approach (RBA)

The Risk-Based Approach (RBA)

Risk assessment

- Risk assessment is the basis of any effective risk-based AML/CFT regime – in particular for allocating resources or applying additional safeguards to the highest-risk areas
- Countries are required to identify, assess and understand their ML/TF risks
- Financial institutions and DNFBPs are required to identify, assess and understand their ML/TF risks

The Risk-Based Approach (RBA)

National risk assessment

- Based on practical, comprehensive and up-to-date understanding of the threats
- Joint effort between relevant ministerial bodies, supervisors, law enforcement authorities, FIU, regulators, financial institutions, etc.
- Up-to-date and accurate information and intelligence enabling relevant authorities to make well-informed judgments
- In-depth analysis of the national circumstances
- Dissemination of results and information sharing with all stakeholders

The Risk-Based Approach (RBA)

An AML/CFT risk assessment should consider:

- Threats
  - Proceeds-generating crime in the country
  - Cross-border flows of illicit finance
  - Active terrorist groups
- Vulnerabilities
  - The nature, scale and complexity of the financial sector
  - The types of financial products and transactions normally undertaken
  - The regulatory environment and level of compliance
- Consequences
  - How much harm will be done if illicit funds are laundered successfully – by criminals? – or by terrorists?

The Risk-Based Approach (RBA)

Specific obligations for FIs and DNFBPs

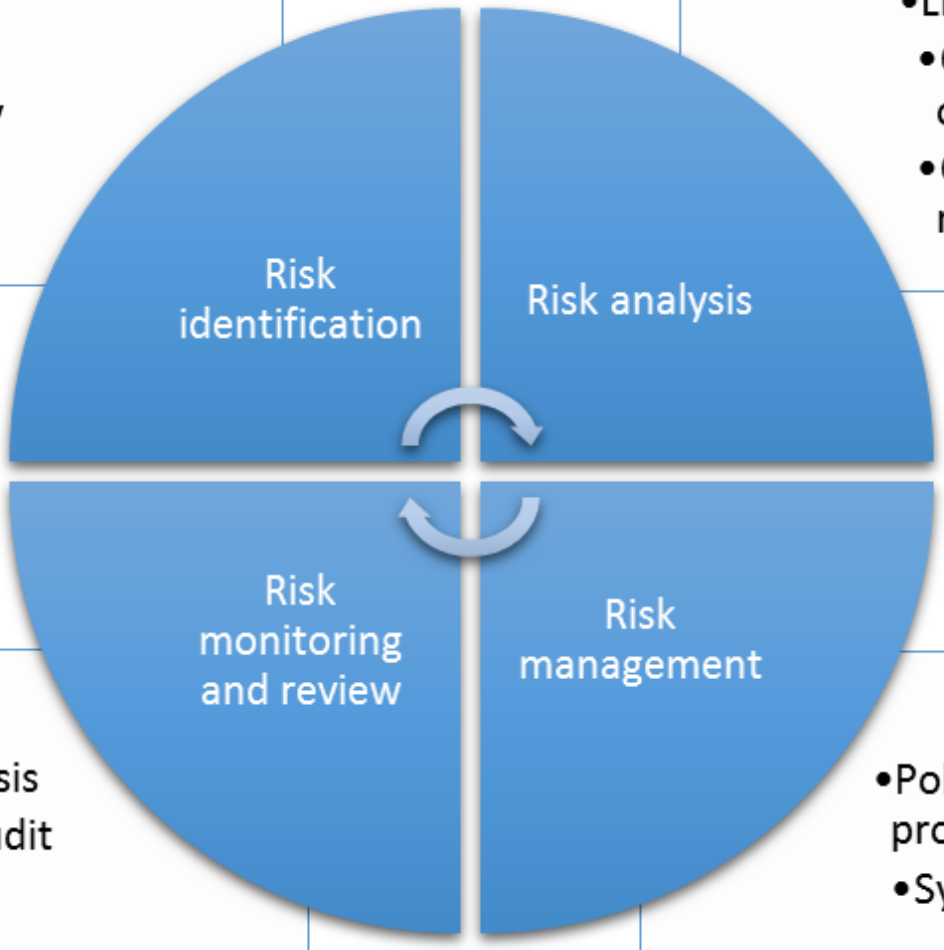
- Updated and documented risk assessment, in accordance with nature and scale of business
- Relevant policies and procedures to manage and mitigate risks, approved by senior management, consistent with national requirements and guidance from relevant national authorities

- Higher-risk → Enhanced measures must be applied
- Lower-risk → Simplified measures may be allowed by countries

Risk assessment process

- Business operations
- Countries
- Customers, delivery channels
- Products, services, transactions

- Likelihood & impact
- Chance of risk occuring
- Cost or damages if risk occured



- Review of risk analysis
- Compliance and audit programs

- Policies and procedures
- Systems and controls

Thank you

For more information please refer to FATF website:
WWW.FATF-GAFI.ORG