FINANCIAL SERVICES COMMISSION

**17-June-2019** **REF: AML-2019/2**

**REGULATORY REMINDER**

**RISK BASED ANTI-MONEY LAUNDERING (AML)**
**AND COUNTERING FINANCING OF TERRORISM (CFT) PROGRAMME**

## 1.0 THE EXISTING REGULATORY ENVIRONMENT

1.1 The Anti-Money Laundering and Financing of Terrorism (**AML/CFT**) Guidelines (**Guidelines**) issued by the Financial Services Commission (**Commission**) requires financial institutions **(FIs**) to develop risk based programmes against money laundering (**ML**) and terrorism financing (**TF**).

1.2 This should be read in conjunction with the Guidelines issued for Commission regulated FIs on anti-money laundering and anti-terrorism financing.

## 2.0 FATF RECOMMENDATION 1

2.1 The revised FATF Recommendations 1 advises that *"FIs should be required to take appropriate steps to identify and assess their money laundering and terrorist financing risks".* FIs *"should document those assessments in order to be able to demonstrate their basis, keep these assessments up to date, and have appropriate mechanisms to provide risk assessment information to competent authorities".*

## 3.0 IDENTIFICATION AND ASSESSMENT OF RISKS

3.1 The risk-based approach includes an assessment of the risk posed by the nature, size and complexity of the FI, the implementation of appropriate mitigation measures, and the assignment of risk ratings to clients.

3.2 A risk assessment is the first step you should take before developing your AML/CFT programme. **Your programme should be based on your risk assessment** and address two main risks: business risk and regulatory risk.

3.3 Regulatory risk is associated with failure to meet your obligations under the Money Laundering and Financing of Terrorism (Prevention and Control) ACT, 2011-23 **(MLFTA)** and the Guidelines.

3.4 Business risk is the risk that the FI may be used for ML/TF. FIs should assess the following risks in particular:

1) customer risks;
2) products or services risks;
3) business practices and/or delivery channels risks; and
4) geographical or jurisdictional risks.

3.5 The risk assessment should also consider the following risk components, where relevant:

1) Governance and oversight;
2) Know Your Customer and Customer Due Diligence;
3) Ongoing monitoring;
4) Name screening and sanctions screening;
5) Suspicious transactions reporting (STR);
6) Record keeping and data management;
7) Staff training; and
8) Risk rating Framework.

3.6 FIs should adopt risk assessment policies and procedures appropriate to their size, nature and complexity. For each of the areas appended above in Section 3.4 and 3.5, the risk assessment should address the following elements:

1) inherent risk;
2) mitigating controls; and
3) residual risk.

3.7 An independent AML/CFT audit of the FI **should be conducted annually** and the results submitted to the Commission. FIs should be prepared to demonstrate and explain the adequacy and effectiveness of their procedures, policies and controls to the Commission.

**4.0 MEASUREMENT OF RISK**

4.1 FIs may determine the most appropriate way to categorize risk, based on the nature and size of the business and the types of ML/TF risk identified from their risk assessment. At their discretion, institutions can apply their own categorization for risk, however high, medium and low ratings typically used by entities.

4.2 FIs should rationalise the criteria used for rating and ranking risks, and address ML/TF risk factors that are unique to specific business lines, customer segments, jurisdictions or any other more general risk factors. FIs should periodically review their risk categories as typologies evolve on the practices by money launderers and terrorists.

4.3 FIs should develop and implement a risk rating framework which is approved by its Board of Directors as being appropriate and capable of assessing the level of potential risk each client relationship poses to the FI.

4.4 The risk rating framework may consider the following risk matrix to obtain a risk score.

| **Likelihood** | | | | |
|---|---|---|---|---|
| Very Likely | Medium<br>2 | High<br>3 | Extreme<br>4 |
| Likely | Low<br>1 | Medium<br>2 | High<br>3 |
| Unlikely | Low<br>1 | Low<br>1 | Medium<br>2 |
| | Minor | Moderate | Major |
| | **Impact** | | |

4.5 **The review of the risk rating for high risk customers should be undertaken more frequently than for other customers**, and where appropriate, a determination should be made by senior management as to whether the relationship should be continued. All decisions regarding high risk relationships and the basis for these decisions should be documented.

## 5.0 RISK MITIGATION

5.1 Senior management and the Board should establish the risk tolerance of FIs. Consideration should be given to whether the FI has sufficient capacity and expertise to effectively manage the established risk tolerance.

5.2 Risk mitigation measures and controls should be commensurate with the risk identified in its risk assessment, inclusive of the risk tolerance of the FI, the risk rating of its customers, products and services and jurisdictional exposure.

5.3 Enhanced measures are required when a FI finds high risks based on its own criteria, whereas simplified measures are allowed when the FI finds lower risks.

## 6.0 RISK MONITORING

6.1 FIs should have systems for on-going monitoring of the risks identified and assessed and update their framework as appropriate to suit the change in risks. Changes may result from changes in customer conduct, development of new technologies, new embargoes and new sanctions.

6.2 FIs should continue to assess the effectiveness of their risk mitigation procedures and controls, and identify areas for improvement, where needed. Areas for on-going consideration include:

1) changes in relevant laws or regulatory requirements;
2) the ability to identify changes in a customer profile or transaction activity/behaviour;
3) the potential for abuse of products and services;
4) changes in typologies;
5) feedback from the Commission or law enforcement feedback, and
6) the adequacy of staff training and awareness.

## 7.0 DOCUMENTATION

7.1 FIs should document their risk based approach, inclusive of the risk assessment, external and internal audits, relevant policies, procedures, review results and mitigation strategies.

7.2 Documentation should clearly show:

1) the risk assessment system including how the FI assesses and rates ML/TF risks;
2) the implementation of appropriate systems and procedures, in light of its risk assessment;
3) enhanced and simplified due diligence requirements;
4) how the FI monitors and, as necessary, improves the effectiveness of its systems and procedures; and
5) the reporting arrangements to senior management on the results of ML/TF risk assessments and the risk based approach.

## 8.0 RISK BASED APPROACH FRAMEWORK

**Risk identification**

- Identify the main ML/TF risks:
- customers
- products & services
- business practices/delivery methods
- countries you do business with
- Identify the main regulatory risks

**Risk assessment/measurement**

- **Measure the size & importance of risk:**
- likelihood – chance of the risk happening
- impact – the amount of loss or damage if the risk happened
- likelihood X impact = level of risk (risk score)

**Risk Mitigation**

- **Manage the business risks:**
- minimise and manage the risks
- apply strategies, policies and procedures

- **Manage the regulatory risks:**
- put in place systems and controls
- carry out the risk plan & AML/CTF program

**Risk monitoring and review**

- monitor & review the risk plan
- develop and carry out monitoring process
- keep necessary records
- review risk plan and AML/CTF program
- do internal audit or assessment
- do AML/CTF compliance report