4

Financial Services Commission
Mauritius

Effective Customer Risk Assessment

30 December 2013

1. Introduction

The Financial Services Commission (the 'Commission') has obligations under the Financial Services Act 2007 (the 'FSA') and the Financial Intelligence and Anti-Money Laundering Act 2002 (the 'FIAMLA') to supervise all its licensees, including Management Companies ('MCs'). Over the last two years, the Commission has conducted on-site inspections for MCs. During this exercise, it has been noted that there are deficiencies in the internal control system of MCs, especially in relation to Anti Money Laundering and Combating the Financing of Terrorism (AML/CFT).

Given the nature of activities of MCs, AML/CFT is of particular importance and relevance for the Commission, as regulator of the non-banking financial services sector and global business sector. According to the Financial Action Task Force (the 'FATF'), MCs are classified as a category of Designated Non-Financial Businesses and Professions (DNFBPs), i.e. Trust and Company Service Providers (TCSPs). The new FATF Recommendations provides clearly the obligations of TCSPs. In the Mauritian context, the FIAMLA, Regulations or guidelines made thereunder and the FSC Code on the Prevention of Money Laundering and Terrorist Financing (the 'FSC Code') set out the duties and obligations of MCs in terms of the AML/CFT requirements.

The FATF Report – Money Laundering Using Trust and Company Service Providers – issued in October 2010 provides a snapshot of the risks and vulnerabilities in the activities of TCSPs. TCSPs indeed play a key role in the economy as intermediaries, providing an important link between financial institutions and many of their customers. However, it is clear that MCs must have a robust and effective AML/CFT framework such that there is adequate mitigation of the risks and vulnerabilities in their businesses.

The objective of this 'Information Booklet' is to provide MCs with a framework which can be adopted to operate within a risk-based environment. It is intended to facilitate MCs in the development of their internal controls systems with a view to discharge their legal obligations in an effective and proactive manner.

2. Building an Effective AML/CFT Programme

The purpose of an effective AML/CFT programme for a MC is to ensure that there are sufficient checks and a high level of transparency so that their businesses are not used for money laundering and terrorist financing purposes. There are different elements that must be considered as a basis for an effective AML/CFT programme, for instance, legal compliance, reputation, protection from criminal liability, amongst others.

2.1. Know the Law

MCs need to keep track of the changes brought to the relevant legislations so that they are aware of any additional obligations or how the existing ones have been enhanced. Such awareness allows MCs to work on how their systems need to be adapted to fulfil their obligations.

2.2. Define the Risk

It is recommended that MCs identify the potential risks and exposures which may affect their respective business operations. As described in the FATF Guidance on Money Laundering and Terrorist Financing Risk Assessment:

> Risk can be seen as a function of three factors: *threat*, *vulnerability* and *consequence*.
>
> A threat is a person or group of people, object or activity with the potential to cause harm to, for example, the state, society, the economy, etc.
>
> The concept of vulnerabilities as used in risk assessment comprises those things that can be exploited by the threat or that may support or facilitate its activities.
>
> Consequence refers to the impact or harm that Money Laundering (ML) or Terrorist Financing (TF) may cause and includes the effect of the underlying criminal and terrorist activity on financial systems and institutions, as well as the economy and society more generally.

For instance, business risk and regulatory risk can be major challenges for MCs; there is a need to strike the right balance between the commercial rationale and reputation, and the legal obligations to meet the regulatory requirements.

Business risks are those risks encountered during the business operations and may include, inter alia:

- customers, including politically exposed persons (PEPs);
- products and services;
- business practices/delivery methods;
- countries with or in which business is conducted; and
- different AML/CFT legislation.

Regulatory risks refer to those risks of not complying with the AML/CFT requirements set out under the legislations and may include, for instance:

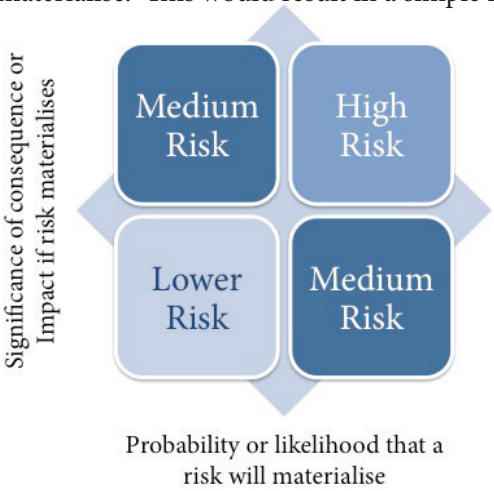
- not having an AML/CTF programme;
- not appointing a Money Laundering Reporting Officer;
- customer verification performed incorrectly;
- failing to report suspicious matters;
- failing to train staff adequately; and
- not doing an AML/CTF compliance report.

Therefore, MCs need to consider where and with whom they are doing business. For instance, the use of introducers by MCs would factor heavily in the risk assessment. MCs should also know what are the risks and vulnerabilities in offering a wide range of products and services, as well as in the markets in which they are operating.

As required under the FSC Code, MCs must make an initial assessment of the risk to which they will be exposed as a result of the business relationship. Depending on the operations of a MC, other risks can also be identified.

2.3. Quantify the risk

After identification of the risks, there is a need to assess and quantify the risks. The classic model of risk analysis would imply looking at the likelihood of occurrence and the impact of the consequence of loss or the severity of damage if the risk does materialise. This would result in a simple matrix as follows:



It will be meaningful for MCs to profile and risk rate customers and assets holistically based on risk attributes including customer geography, business structure, sources of funds, business type, products and services used, and other factors.

2.4. Manage the risk

Now that the risks have been identified and quantified, there is a need to develop adequate measures to manage the risk. A risk management programme will entail putting in place people, processes and controls adequate to the risks in order to meet the objectives of the AML/CFT programme.

2.4.1. Design

As set out in the FSC Code, MCs are required to conduct customer due diligence (CDD) on all their customers. MCs must therefore ensure that their internal control systems are designed in such a way that they allow to:

- clearly identify the roles and responsibilities of their staff and management in the AML/CFT programme;
- collect CDD documentation, which will help MCs to 'know' the customer and therefore enable the MCs to categorise their customers according to their risks (e.g. High Risk, Medium risk and Low risk);
- embed within their systems suspicious transaction/activity controls;
- use an automated system for transaction monitoring, e.g. using thresholds or records matching (e.g. an alert popup when a new or existing customer matches with one of the records in the lists disseminated by the FSC on the United Nations Sanctions Committee Resolutions).

2.4.2. Implement

MCs are required to adopt the prescribed CDD procedures in terms of identification and verification of customers. The following will help implementation of an effective AML/CFT programme:

- Clear policies and procedures established in the internal control systems;
- Proper awareness and training of staff for them to understand how to apply the controls;
- Automated systems to allow MCs to monitor, review and report on any suspicious transaction/activity

Where MCs are not comfortable that the information available is sufficient to understand the business relationship with the customer, the MCs may need to escalate the review to get a full picture of the customer's business. In such cases where the customers represent high-risk relationships, enhanced CDD measures must be applied. MCs may also refer to the FSC Code and to the FATF Guidance on Politically Exposed Persons (PEPs) in terms of the red flags or potential indicators of a high risk business relationship.

However where the initial assessment of the risk determines that a customer does not pose a high risk of money laundering and terrorist financing, MCs may apply simplified or reduced CDD measures. In such cases, information on the customer is usually publicly available.

2.4.3. Test and analyse

Once the system is in place, as provided in the FSC Code, MCs are required to perform independent testing. Controls must be tested regularly and results analysed so as to ensure that the system is actually working properly.

For instance, when Eligible Introducer Certificates are used, MCs need to ensure that testing is conducted to ascertain whether the working arrangement is satisfactory and that the documentation is provided to them in a timely manner.

It is also relevant to test how the communication channel operates when suspicious transactions/activities have been identified.

2.4.4. Report

From the testing performed, any weakness needs to be reported so that appropriate measures are taken by the MCs to remedy the situation.

MCs are also encouraged to file suspicious transaction reports with the FIU as and when there is a need to do so. Reporting by the MCs is not only a statutory obligation but it also helps the MCs in maintaining their reputation.

2.5. Improvement and evolution

The AML/CFT system needs to be continuously updated in the light of additional potential risks, threats and vulnerabilities of the MCs. The system will only be effective when it is adapted to the environment in which it is operating.

Whilst there are changes to legislations, criminals also come up with new methods of countering laws. MCs therefore must keep themselves abreast of new developments and ensure that their AML/CFT system is reviewed accordingly.

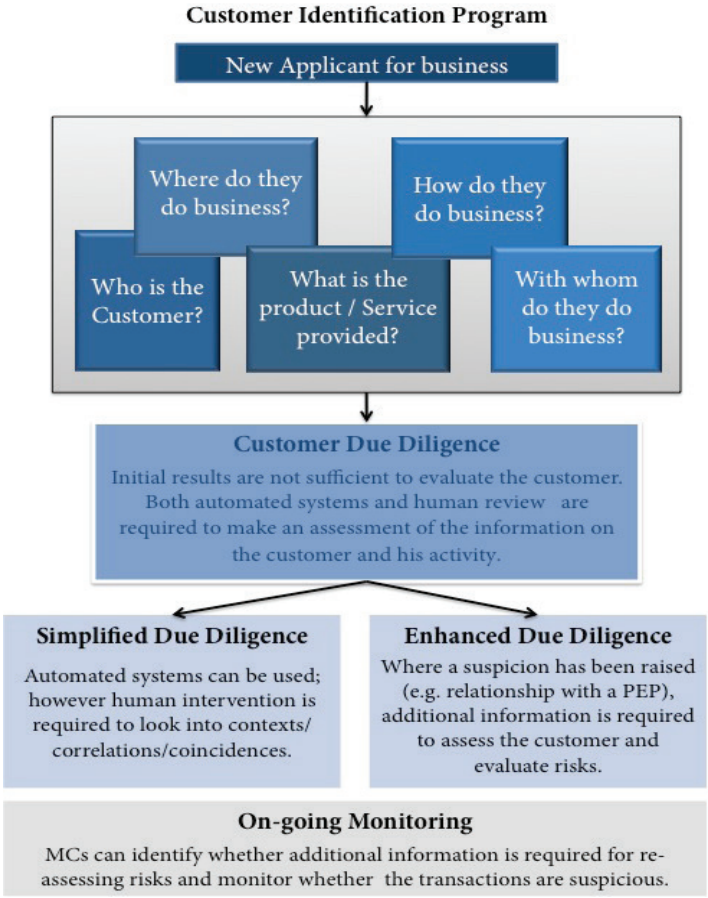
3. **Effective Customer Risk Assessment**

3.1. Customer Identification Program (CIP)

It is necessary to consider the different ML/TF risks that a customer pose to the system when formulating customer identification procedures.

Most customers using the services will be legitimate. However the systems and procedures need to be alert and responsive to instances where a customer's background places him into a category of a higher risk customer. For this reason, it is a requirement to correctly identify a customer before providing the customer with a service (although there are exceptional cases, as provided for in the FSC Code). Failure to correctly identify and verify the customer at the outset may prevent any effective ongoing customer due diligence activity.

Customer identification controls are only part of ensuring that the true identity of a customer is established.


Customer Identification Program
New Applicant for business
Where do they do business?
How do they do business?
Who is the Customer?
What is the product / Service provided?
With whom do they do business?
Customer Due Diligence
Initial results are not sufficient to evaluate the customer. Both automated systems and human review are required to make an assessment of the information on the customer and his activity.
Simplified Due Diligence
Automated systems can be used; however human intervention is required to look into contexts/ correlations/coincidences.
Enhanced Due Diligence
Where a suspicion has been raised (e.g. relationship with a PEP), additional information is required to assess the customer and evaluate risks.
On-going Monitoring
MCs can identify whether additional information is required for re-assessing risks and monitor whether the transactions are suspicious.

3.2. Customer due diligence

Knowing your customer ('KYC') is necessary to determine ML/TF risk that MCs may face when providing a service to that customer. The requirement to establish and verify the identity of a customer before providing a service to that customer is a key obligation of ML/TF. Understanding them, their products, services, market areas, and business can help avoid high-risk situations and potential catastrophe.

Appropriate KYC measures are determined through risk analysis of the customer relationship, covering:

- Who is the customer?
- Where do they do business?
- What are the products/services provided?
- How do they do business?
- With whom do they do business?
- What methods are used to deliver the services?
- Whether the customer operates in foreign jurisdictions that have less stringent AML/CFT legislation or if the country is identified as being at high risk for ML/TF?

3.3. Enhanced due diligence

Enhanced customer due diligence programme must be applied where ML/TF risk is high, or when a suspicious matter reporting obligation arises. In applying enhanced customer due diligence the following may be considered:

- seeking further information from the customer or third-party sources to clarify, update or obtain the customer's KYC information; clarify the nature of the customer's ongoing business with the reporting entity; or consider any suspicion that may be reportable;
- undertaking more detailed analysis of their KYC information;
- verifying or re-verifying KYC information;
- analysing the customer's past transactions and possibly monitoring future transactions.

If due diligence procedures have raised suspicions about a customer or the MC has not been able to have a full picture to allow a categorisation of the customer, additional due diligence is needed. As a result, the customer would be considered as a high-risk customer, who may include a PEP, a family member of a PEP or an associate.
The MC may even consider whether to accept such a business relationship in that the customer may pose too many risks to its business.

3.4. Simplified due diligence

Simplified CDD measures can be applied in cases where there is a demonstrated low ML/FT risk. Examples are set out in the FSC Code. However this should in no case amount to an exemption from or absence of CDD. At the initial stage of the customer identification, the MC may find that such customers would not require further CDD since there are few risks associated to them, e.g. in the case of well-known large public companies. As a result, automated and basic checks may be sufficient unless there are any trigger factors which would indicate the MC that the risk level of that customer has changed.

3.5. On-going monitoring

On-going monitoring is part of a reporting entity's overall CDD obligations. Broadly speaking, CDD involves:

- collecting and verifying initial KYC information; and
- providing ongoing monitoring of customers and their transactions.

Ongoing monitoring, of the entire customer base, is essential in identifying customer risk before it becomes a problem. MCs are required to monitor customers and their transactions on an ongoing basis. AML/CFT programme needs to include systems and procedures that reflect the risk-based approach. This means that high-risk situations will require more attention than low-risk situations.

Two main components of on-going monitoring:

a. Collecting and verifying initial know your customer (KYC) information

   AML/CFT program will need to address whether and in what circumstances further KYC information about customers should be updated or existing KYC information verified. Examples of when this may be necessary include when a significant transaction (for example, in amount, size or volume) takes place or a material change to how the account has been previously operated by the customer.

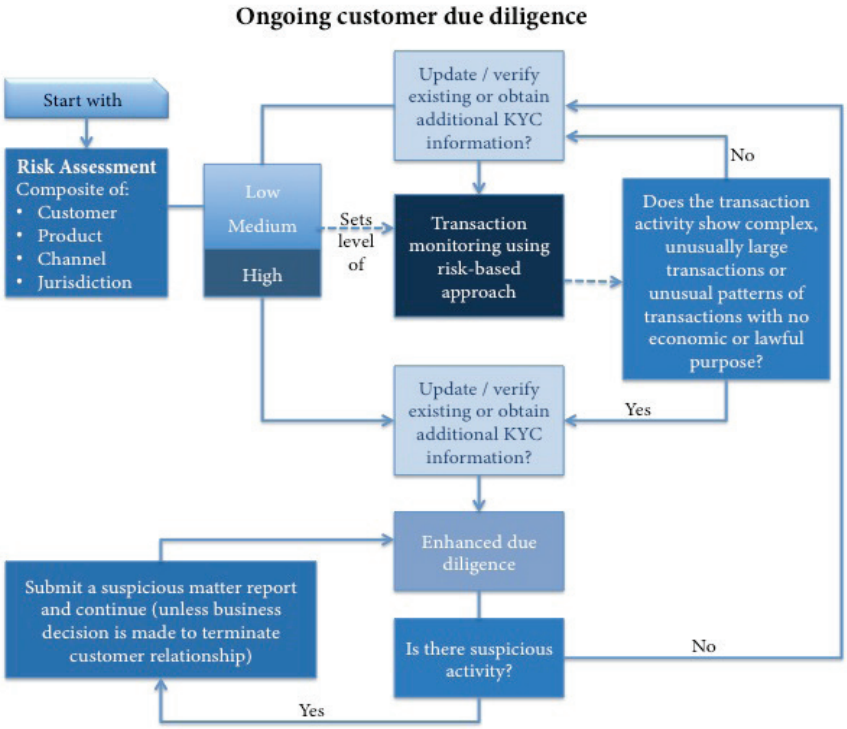
b. Providing ongoing monitoring of customers and their transactions

   AML/CFT programme must include a transaction monitoring program to detect suspicious transactions when they occur.

To identify apparently suspicious transactions, the transaction monitoring program must have regard to complex or unusual large transactions and all unusual transaction patterns where there is no apparent economic or lawful purpose. Examples of these include:

- significant transactions (in terms of amount or volume) for that customer;
- transactions that exceed transaction or amount limits;
- very high account turnover inconsistent with the size of the balance; and
- transactions outside the regular pattern of an account's activity.

The chart below provides a snapshot of the on-going customer due diligence process:



Source: AUSTRAC

4. The Risk Based Approach

The new FATF Recommendation 1 imposes on all countries an obligation to "identify, assess, and understand the money laundering and terrorist financing risks for the country, and should take action, including designating an authority or mechanism to coordinate actions to assess risks, and apply resources, aimed at ensuring the risks are mitigated effectively."

Countries must also require their "designated non-financial businesses and professions (DNFBPs) to identify, assess and take effective action to mitigate their money laundering and terrorist financing risks."

The FATF RBA Guidance for Trust and Company Service Providers has been issued in June 2008 to provide an indication of good practice in the design and implementation of an effective risk-based approach.

In essence, it is a process of identifying exposures to money laundering and terrorist financing risk, and then allocating your resources commensurately to the assessed risk. It accepts that finite resources are available to mitigate risk and enables MCs to focus more on the higher risks areas and less on areas of lower risk.

Therefore the development and implementation of effective AML/CFT controls are pre-requisite to managing the exposure to ML and TF risks.

4.1. Why conduct a Risk Based Assessment?

A solid risk assessment would enable MCs to:

- Develop a compliance program that is generally effective in detecting and deterring money laundering and terrorism financing;
- Act as the foundation against which the MC can demonstrate program adequacy (procedures, training, transaction monitoring, etc);
- Prioritise resources, investments, and implementation schedules;

- Enable risk-based differentiation with respect to due diligence, training and procedures contents, as well as various timelines (testing, member account review, file refresh, etc);
- Identify gaps within the existing program;
- Meet regulatory requirements; and
- Protect your organization.

4.2. Risk Categories

The Risk Categories can be identified as follows:

- Country/geographical risk;
- Customer risk; and
- Product risk.

4.2.1. Country/geographical risk

The location, of where MCs do business with, can impact heavily on the risk matrix. It is crucial that the MCs identify the risks associated with doing business in a particular country or region. For instance, the FATF publishes Statements on a regular basis on high-risk and non-cooperative jurisdictions.

It is recommended that MCs keep themselves updated on the countries being monitored by the FATF. Similarly other international organisations e.g. FATF-Style Regional Bodies, United Nations, IMF, World Bank, Egmont Group of Financial Intelligence Units, may also disseminate information in relation to risks prevailing in some countries.

4.2.2. Customer Risk

With the growing focus on Know Your Customer (KYC), MCs need to rethink on their business relationships and their customer acceptance process. Because there may exist different categories of clients, especially where MCs offer a rich set of products and services, customer acceptance processes should be segmented and detailed for each client category.

Characteristics of each client can provide useful information in assisting a MC to identify those clients that may pose higher risks to its business. Examples may include:

- Politically Exposed Foreign Persons;
- Non face-to-face relationships;
- Members listed in applicable controls/higher risk lists; and
- Organizations with various/complex legal structures including NGOs.

4.2.3. Product Risk

An overall risk assessment should also include but not limited to the risk presented through innovative products and services. For instance, a key element for MCs is establishing the existence of an apparent legitimate business, economic, tax or legal reasons for the structures it has been asked to set up and manage.

Therefore the following should be taken into consideration, amongst others:

- Monitoring of high risk accounts;
- Situations where it is difficult to identify the beneficiaries of trusts;
- Intended use of accounts and large transactions with no apparent economic value or service;
- Third party determinations and the beneficial ownership of companies.

4.3. Internal Controls

In order for MCs to have an effective risk-based approach, the risk-based process must be imbedded within the internal controls of the institutions.

An internal control system includes policies, processes, tasks, behaviours and other aspects of a company and can be summarised as set out below:

- facilitate effective and efficient operation to respond appropriately to operational, financial, compliance and other risks;
- help ensure the quality of internal and external reporting; and

- help ensure compliance with applicable laws and regulations, and also with internal policies with respect to the conduct of business.

Internal control can be analysed into five inter-related components, which also serve as criteria for the effectiveness of the internal control system in supporting the achievement of the separate but overlap with operational, financial reporting and compliance objectives. The components are:

- Control environment – ethical values and competence (quality) of personnel, direction provided by the board and effectiveness of management;
- Risk assessment – identification and analysis of risks relating to the changing regulatory and operating environment, as a basis for determining how such risks should be mitigated and managed;
- Control activities – a diverse range of policies and procedures that help to ensure management directives are carried out;
- Information and communication – effective processes and systems that identify, capture and report operational, financial and compliance-related information in a form and timeframe; and
- Monitoring – a process that assesses the adequacy and quality of the internal control system's performance over time.

Financial Services Commission
FSC House, 54 Cybercity Ebene, Mauritius
Tel: (230) 403 7000 | Fax: (230) 467 7172
E-mail: fscmauritius@intnet.mu | Website: www.fscmauritius.org