Financial Services Commission
Mauritius
Insurance Workshop on AML/CFT

Presented by: Ms Clairette AH-HEN

Date: 27 August 2014
Insurance Workshop on AML/CFT

Agenda

- Legal Framework
- Assessment by International Organisations
- Role of FSC
- Insurance Sector Vulnerabilities
- FSC AML/CFT Code
  - Major requirements
- Risk Based Approach
  - AML/CFT Programme
  - Effective Customer Risk Assessment
Legal Framework
Legal Framework

**Financial Services Act 2007 [Section 6(g) – Functions of the FSC]**

• “To carry out investigations and take measures to suppress illegal, dishonorable and improper practices, market abuse and financial fraud [including ML] in relation to any activity in the financial services sector and global business sectors”

**Insurance Act 2005 – Section 3(2)(d)**

• “Reducing as far as is reasonably possible the risk that the insurance business is used in furtherance of, or for a purpose connected with, a financial crime.”

**FIAML Act – Section 18(1c)**

• “The Financial Services Commission shall supervise and enforce compliance by financial institutions with the requirements imposed by this Act, regulations made under this Act and such guidelines as it may issue under paragraph (a).”
Assessment by International Organisations
Assessment by International Organisations

Financial Action Task Force
- 40 Recommendations – Feb 2012

International Association of Insurance Supervisors (IAIS)

IMF/World Bank Assessment
- Financial Sector Assessment Program
  - Last Assessment – Report issued in Dec 2008

Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG)
- Continuous monitoring of progress made on the recommendations
Role of FSC
Role of FSC

Issue of Guidelines – FSC AML/CFT Code

On-site Inspection
- Check adherence to FSC Code

Off-site Supervision
- Ensure proper appointment and submission of documents

Enforcement Actions in case of non-compliance
Insurance Sector Vulnerabilities
Insurance Sector Vulnerabilities

Vulnerabilities depend on factors

- complexity and terms of the contract,
- distribution,
- method of payment (cash or bank transfer)

Duty of vigilance:

- customer due diligence (CDD), including underwriting checks and verification of identity;
- recognition and reporting of suspicious customers/transactions; and
- provisions affecting the organisation and the staff of the insurer, such as a compliance and audit environment, keeping of records, the recruitment of staff and training.
FSC AML/CFT Code
FSC AML/CFT Code

FSC Code issued in March 2012

- Applicable to all Licensees
- Licensees defined under the FIAMLA, including insurers, insurance brokers, insurance agents and salespersons

FSC Code – Statement of minimum criteria

Regular updates of the FSC Code (from 2005 to 2012)
- Non-compliance with the Code exposes the licensee to regulatory action including a direction under section 7(1)(b) of the FSA to observe the Code.

Failure to comply with the direction may lead to criminal action and to regulatory action.
FSC AML/CFT Code

Major Requirements

- Internal controls and MLRO
- Customer Due Diligence
- High risk and low risk relationships
- On-going monitoring and reporting suspicious transaction
- Training and culture
- Record keeping
Risk Based Approach
AML/CFT Programme

The primary reasons for an effective AML-CFT programme include legal compliance, reputation management, protection from criminal prosecution and just not wanting to handle dirty money.

**Know the Law**
- Keeping up with ever-changing laws and regulations about financial transactions and money laundering possibilities

**Define the Risk**
- Define corporate roles & responsibilities
- Determine risk-based due diligence
- Designate risk categories
- Build suspicious activity controls

**Quantify the Risk**
- Quantitative impact of defined risks
- Understand how operating locations affect risk
- Profile and risk rate customers and assets

**Manage the Risk**
- Develop a programme of people, processes and controls proportional to the quantified risks which can ensure compliance, visibility and protection

**CONSTANT IMPROVEMENT**
- Continually capture and update the understanding of threats and system weaknesses to influence continued evolution of an effective AML programme

**DESIGN**
- Establish policies, procedures, and operating models
- Conduct training
- Utilise technology to monitor, review, escalate, and report suspicious activities

**IMPLEMENT**
- Regularly test controls
- Monitor personnel
- Evaluate data
- Ensure proper channeling communication of suspicious activity

**TEST & ANALYSE**
- Report suspicious activity and system weaknesses for analysis
- File Suspicious Activity Reports (with FIU)

**REPORT**
- Know the exposure - threats posed by your operations, products & services, markets and different customer types
Effective Customer Risk Assessment

Customer Identification Program (CIP)

- **Who is the Customer?**
- **Where do they do Business?**
- **What is the Product/Service?**
- **How do they do Business?**
- **With whom do they do Business?**

**CUSTOMER DUE DILIGENCE**

- If initial due diligence yields suspicious results or the information obtained is not sufficient to evaluate the risk of a customer, an escalated review is applied which may include both automated and additional human review of both the customer activity and other information.

**ENHANCED DUE DILIGENCE**

- If due diligence procedures have either raised suspicions about a customer or have not painted as full a picture as needed to evaluate risk or the customer as a class (e.g. Politically Exposed Persons ("PEPs")) represents a higher degree of risk, additional due diligence is needed.
- Further investigation may lead to the decision that the customer represents too much risk to the business.

**SIMPLIFIED DUE DILIGENCE**

- Each customer will undergo some measure of due diligence, beginning with initial due diligence processes beyond CIP.
- Customers with few risk factors, for example well known large public companies and customers utilizing some types of low-risk products or services, may only require a simplified due diligence process.

**ONGOING MONITORING**

- Once the customer has been taken on board, ongoing monitoring is essential in identifying Customer Risk before it becomes a problem.
**Category of Risk Profile for Licensees**

Licensees will fall into one of the following risk profile:

<table>
<thead>
<tr>
<th>Monitoring</th>
<th>Low</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remediation</td>
<td>Low</td>
<td>High</td>
</tr>
</tbody>
</table>

This would apply to Licensees who are undergoing a change in both business and control environment either as a result of the changing business plan or to correct control deficiencies.

These Licensees are the ones that the FSC will be most concerned about and where close monitoring, focussed visits and regular contacts are required.

<table>
<thead>
<tr>
<th>This could apply to start-up companies.</th>
<th>Licensees where a remediation programme is necessary to improve their risk profile.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Licensees that have strong control environment supported by good governance as well as a stable business plan and who generally are lower impact entities.</td>
<td>Licensees that are making improvements to their control environment and regulatory compliance arrangements, and are operating in a stable business environment.</td>
</tr>
</tbody>
</table>

**Remediation**
Any Questions
Conclusion

- The Insurance Sector remains possible targets for money launderers
- Build compliance culture
- Uphold the reputation of the jurisdiction
- Strike the right balance of regulation
THANK YOU
FOR YOUR KIND ATTENTION

Vision

“To be an internationally recognised Financial Supervisor committed to the sustained development of Mauritius as a sound and competitive Financial Services Centre”