GUIDELINES ON THE MEASURES FOR THE PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM FOR DEALERS UNDER THE FINANCIAL INTELLIGENCE AND ANTI MONEY LAUNDERING ACT 2002

Amended July 2020
**DISCLAIMER**

These Guidelines are intended to provide assistance to dealers under the Financial Intelligence and Anti Money Laundering Act (FIAML) hereinafter referred to as Dealers) in meeting their obligations under the (FIAML, United Nations(Financial Prohibitions, Travel Ban and Arms Embargo) Sanctions Act 2019 (UN Sanctions Act) and the Financial Intelligence and Anti Money Laundering Regulations 2018 (FIAML Regulations). If you are unsure about your obligations in a given case, you should consider taking independent legal advice.

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AML/CFT</td>
<td>Anti-Money Laundering and Combating the Financing of Terrorism</td>
</tr>
<tr>
<td>CDD</td>
<td>Customer Due Diligence</td>
</tr>
<tr>
<td>CO</td>
<td>Compliance Officer</td>
</tr>
<tr>
<td>DNFBPs</td>
<td>Designated Non-Financial Businesses and Professions</td>
</tr>
<tr>
<td>EDD</td>
<td>Enhanced Due Diligence</td>
</tr>
<tr>
<td>ESAAMLG</td>
<td>Eastern and Southern Africa Anti-Money Laundering Group</td>
</tr>
<tr>
<td>FATF</td>
<td>Financial Action Task Force</td>
</tr>
<tr>
<td>FIAML</td>
<td>Financial Intelligence Anti-Money Laundering Act</td>
</tr>
<tr>
<td>FIU</td>
<td>Financial Intelligence Unit</td>
</tr>
<tr>
<td>ML</td>
<td>Money Laundering</td>
</tr>
<tr>
<td>NRA</td>
<td>National Risk Assessment</td>
</tr>
<tr>
<td>PCPs</td>
<td>Policies, Controls and Procedures</td>
</tr>
<tr>
<td>PEP</td>
<td>Politically Exposed Person</td>
</tr>
<tr>
<td>PF</td>
<td>Proliferation Financing</td>
</tr>
<tr>
<td>STR</td>
<td>Suspicious Transaction Report</td>
</tr>
<tr>
<td>TF</td>
<td>Terrorism Financing</td>
</tr>
</tbody>
</table>
# Table of Contents

1. Introduction ......................................................................................................................... 1

2. Money Laundering and Financing of Terrorism and Proliferation ........................................ 6

3. Risk-Based Approach ............................................................................................................ 8

4. Internal Controls ................................................................................................................... 20

5. Preventive Measures ............................................................................................................ 26

6. Terrorist Financing Offences ................................................................................................. 43

7. ML/TF Indicators for Dealers ............................................................................................... 46

Annex 1. Risk Assessment Form for Dealers ........................................................................... 48

Annex 2: Template for AML/CFT Policies and Procedures ......................................................... 55
1 Introduction

Money laundering, terrorism and proliferation financing have far reaching consequences for a country’s financial system and economy. With these crimes becoming increasingly cross border in nature, jurisdictions must equip themselves to protect the integrity of their financial systems and must also be prepared to deal with any abuses which are encountered. In order to achieve this, there are several building blocks which are required. The first is a sound and robust legal framework, which empowers institutions and lays down the obligations of all parties concerned. The second is an open and collaborative approach between AML/CFT supervisors and the reporting persons that they regulate. Additionally, there must be a willingness from the sectors which are regulated to understand their obligations and to accept that they also have to contribute to the fight against ML and TF. Against this background, the FIU, as the AML/CFT regulator for dealers, firmly believes that one crucial way through which ML and TF can be curbed, is through the implementation of strong controls, policies and procedures by dealers. These act as a line of defence in ensuring that the jewellery sector does not become a haven for criminals. The purpose of these guidelines is to assist dealers in establishing strong systems and in becoming partners in the fight against ML and TF. Its objective is also to help the sector in understanding its AML/CFT obligations.

1.1 The Mauritian AML/CFT Legislative Framework

Mauritius has taken significant steps to ensure that it has a robust AML/CFT legal framework which is aligned with international standards. The FIAMLA was enacted in 2002 and provided for several of the key requirements of a strong AML/CFT system. It has been amended to ensure that Mauritius meets its international obligations. Among other things, the FIAMLA makes provision for an independent FIU, the obligation of filing suspicious transaction reports, CDD obligations as well as a framework for the AML/CFT supervision of Designated Non-Financial Businesses and Professions (DNFBPs).

In 2018, the FIAML Regulations 2018 were made and revoked the then 2003 FIAML Regulations. The 2018 Regulations make extensive provision in relation to the measures which must be put in place by reporting persons (which includes dealers) to ensure that they are complying with the requirements of the law and that they are taking the required steps to safeguard their businesses from ML/TF abuses.
(henceforth referred to as the ‘UN Sanctions Act’) was also passed in May 2019. This act enables Mauritius to implement the measures under all the United Nations Security Council Resolutions and deal with other matters of international concern, and to give effect to Article 41 of the Charter of the United Nations.

Copies of the above legislations are available on the FIU’s website: www.fiumauritius.org.

1.2 Purpose and Scope of the Guidelines

The Jewellery sector may become a preferred choice for criminals for hiding illicit gains. This arises because of a number of factors such as the relatively high monetary value of the transactions conducted, the appreciation of the assets’ value over time, the portability of the products and the opportunity to conceal ownership.

As per the findings of the National Risk Assessment (2019) Public Report, the following factors make the sector inherently vulnerable to money laundering:

(a) the client-base profile of the sector, which includes domestic politically exposed persons, high-net worth individuals, non-resident clients and clients with criminal records;
(b) the use of cash – the sector has been characterized by a high volume of low value transactions;
(c) the anonymous use of the product - where jewellery is purchased by a third party on behalf of the true owner; and
(d) the relative difficulty of tracing transaction records as transactions are conducted without complying with the prescribed due diligence and disclosure requirements.

Dealers are involved in the vast majority of jewellery transactions in Mauritius and, therefore, can play a key role in detecting money laundering and financing of terrorism and proliferation schemes involving this industry. Given that they are in direct contact with clients (either buyer and/or sellers), they are well placed to detect any suspicious transaction/activity.

This document has been issued pursuant to section 10(2)(ba) of the Financial Intelligence and Anti Money Laundering Act (FIAMLA) 2002. They are intended to assist dealers in complying with their obligations in relation to the prevention, detection and reporting of money laundering, financing of terrorism and proliferation. Through compliance with their obligations, dealers can ensure that their businesses are not misused by money launderers or those financing terrorism or proliferation.
1.3 Businesses and Individuals covered by the Guidelines

This guideline is addressed to the following:

- Dealers under the FIAMLA who engage in any transaction of at least 500,000 rupees in total, whether the transaction is executed in a single operation or in several operations which appear to be linked.

Under the FIAMLA, the following terms are defined:

“Dealer in jewellery, precious stones or precious metals” means –

(a) a person who deals in jewellery, precious stones or precious metals; and
(b) includes a person who –
   (i) manufactures, processes, buys, sells, imports or exports jewellery or supplies jewellery for sale;
   (ii) processes, buys, sells or imports precious metals or exports melted precious;
   (iii) or, processes, buys, sells or imports precious stones.

“Jewellery” means any article made of a precious metal or its alloy, and which exceeds one gramme.

“Precious metal” means

(a) gold, silver, platinum or palladium; and

(b) includes any object which is composed of gold, silver, platinum or palladium.

“Precious stone” means diamond, sapphire, ruby, emerald, alexandrite or tanzanite.

1.4 The Financial Action Task Force (FATF)

The Financial Action Task Force (FATF) was established in 1989 by the G7 countries. It is an inter-governmental body whose purpose is to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, financing of terrorism and other related threats to the integrity of the international financial system.
As a member of the Eastern and Southern Africa Anti-Money Laundering Group, Mauritius has made the commitment to implement these standards into its domestic AML/CFT framework.

1.5 The Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG)

The ESAAMLG was founded in 1999 and its main objective is to ensure that its Members comply with the FATF standards. Assessment for compliance with the FATF Recommendations is done through the Mutual Evaluation Process following which a Mutual Evaluation Report (MER) is prepared and posted on the ESAAMLG’s website. The most recent MER of Mauritius can be accessed on the FIU Website¹.

1.6 Compliance with Guidelines and Enforcement

As the AML/CFT regulator for the jewellery sector, the FIU is mandated to ensure compliance by the latter with the FIAMLA, the UN Sanctions Act, and any regulations and guidelines issued under these Acts. Following legal amendments made in May 2019, FIU has been further empowered, and provided with significant powers to enforce compliance by the sector. The FIU is now able to:

- give directions to members (in the present case this means Dealers) falling under their respective purview;
- require members to submit a report on corrective measures it is taking to ensure compliance with the relevant legislation;
- take administrative sanctions as provided for by FIAMLA;
- revoke or cancel licences, approvals or authorization as the case may be; and
- request information or records from its members in the discharge of its functions.

1.7 The Financial Intelligence Unit (FIU)

The FIU Mauritius was set up in August 2002 under the provisions of section 9 of the FIAMLA. It is the central agency in Mauritius responsible for receiving, requesting, analyzing and disseminating to the investigatory, supervisory authorities², Registrars and overseas FIU disclosures of information.

¹http://www.fiumauritius.org/English/Documents/ESAAMLG%20DOCS/Second%20Round%20MER%20of%20Mauritius-July%202018.pdf
²Investigatory authorities" include the Commissioner of Police, the Director, The Mauritius Revenue Authority, the Enforcement Authority and the ICAC and "supervisory authorities" include the Bank of Mauritius, the Financial Services Commission, the GRA,
regarding suspected proceeds of crime and alleged money laundering offences as well as the financing of any activities or transactions related to terrorism to relevant authorities.
2. Money Laundering and Financing of Terrorism and Proliferation

2.1 Money Laundering

Money laundering is the process intended to disguise the illegal origin of proceeds of crime in order to make them appear legitimate. If undertaken successfully, it allows criminals to maintain control over proceeds of criminal activities and, ultimately, provide a legitimate cover for these activities. The process is often carried out in three stages:

(1) Placement

This initial stage involves the introduction of criminally tainted money into the financial system. The launderer seeks to introduce illegal proceeds into the financial system by, for example breaking up large amounts of cash into less conspicuous smaller sums that are then deposited directly into a bank account, or by purchasing a series of monetary instruments (e.g. cheques etc.) that are then collected and deposited into accounts at another location.

(2) Layering

The layering stage is the dissociation of the dirty money from their source through a series of transactions to obscure the origins of the proceeds. These transactions may involve different entities such as companies and trusts as well as different financial assets such as shares, securities, properties or insurance products. It is the separation of benefits of drug trafficking or criminal conduct from their source by creating layers of financial transactions designed to disguise the audit trail. Illustratively, the launderer may engage in a series of conversions or movements of the funds to distance them from their source. (e.g. buying and selling of stocks, commodities or properties, buying precious metals or stones with cash, taking out and repaying a loan, use of gatekeepers and their services to buy and sell assets etc). The funds might even be channelled through the purchase and sale of investment instruments, or the launderer might simply wire the funds through a series of accounts at various banks across the globe. This use of widely scattered accounts for laundering is especially prevalent in those jurisdictions that do not co-operate in anti-money laundering investigations. In some instances, the launderer might disguise the transfers as payments for goods or services or use gatekeepers to carry out such transactions, thus giving them a legitimate appearance.
(3) Integration

The integration stage is the use of the funds in the legitimate economy through for instance, investment in real estate or luxury assets. Essentially, it is the provision of apparent legitimacy to benefits of drug trafficking or other illegal activities. If the layering process has been successful, the integration schemes thus place the laundered funds back into the economy so that they re-enter the financial system appearing as legitimate business funds. They can then be used for legitimate purchase of luxury goods, real estate and soon.

2.2 Financing of Terrorism

Financing of terrorism is the process by which funds are provided to an individual or group to fund terrorist activities. Unlike money laundering, funds can come from both legitimate sources as well as from criminal activity for the financing of terrorism. Funds may also originate from personal donations, profits from businesses and charitable organizations but all the funds are actually used to finance terrorism. Funds may come, as well as from criminal sources, such as the drug trade, the smuggling of weapons and other goods, fraud, kidnapping and extortion.

Unlike money laundering, which precedes criminal activity, with financing of terrorism, it is possible to have fundraising or a criminal activity generating funds prior to the terrorist activity actually taking place. However, similar to money launderers, those financing terrorism also move funds to conceal their source of those funds. The motive is to prevent leaving a trail of incriminating evidence.

2.3 Proliferation Financing

Proliferation of weapons of mass destruction ("WMDs") can be in many forms, but ultimately involves the transfer or export of technology, goods, software, services or expertise that can be used in programmes involving nuclear, biological or chemical weapons, and their delivery systems (such as long-range missiles). Proliferation of WMD financing is an important element and, as with international criminal networks, proliferation support networks may use the international financial system to carry out transactions and business deals. Unscrupulous persons may also take advantage of the potential profits to be made by facilitating the movements of sensitive materials, goods, technology and expertise, providing seemingly legitimate front organizations or acting as representatives or middlemen.
3. Risk-Based Approach

3.1 Adopting a Risk-Based Approach

Recommendation 1 of the FATF focuses on assessing risks and applying a risk-based approach. Based on the findings of its first national ML and TF risk assessment, which was completed in August 2019, the ML risk associated with the Jewellery sector was found to be Medium-High. The level of ML threat was rated Medium. The main predicate offence associated with the sector was jewellery theft. A possible link between the sector and drug trafficking was also identified. Alternatively, the following factors make the sector inherently vulnerable to money laundering:

(a) the client-base profile of the sector, which includes domestic politically exposed persons, high-net worth individuals, non-resident clients and clients with criminal records;
(b) the use of cash – the sector has been characterized by a high volume of low value transactions;
(c) the anonymous use of the product- where jewellery is purchased by a third party on behalf of the true owner; and
(d) the relative difficulty of tracing transaction records as transactions are conducted without complying with the prescribed due diligence and disclosure requirements.

It is an obligation for dealers to identify, assess and understand their ML/TF risks pursuant to section 17 of FIAMLA. It is highlighted that dealers should take into account the outcome of the National Risk Assessment when applying CDD measures in relation to each customer.

---

3 For the purpose of assessing money laundering and terrorism financing risks, risk is defined as a function of 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. In the ML/TF context this includes criminals, terrorist groups and their facilitators, their funds, as well as past, present and future ML or TF activities.
- Vulnerabilities comprise those things that can be exploited by the threat or that may support or facilitate its activities. In the ML/TF risk assessment context, looking at vulnerabilities means focusing on, for example, the factors that represent weaknesses in AML/CFT systems or controls or certain features of a country. They may also include the features of a particular sector, a financial product or type of service that make them attractive for ML or TF purposes.
- Consequence refers to the impact or harm that ML or 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.

4 The public version of the NRA report may be accessed here: http://www.fiumauritius.org/English//DOCUMENTS/NRA%20FINAL%20REPORT.PDF
A risk-based approach also requires dealers to have systems and controls that are commensurate with the specific risks of money laundering and financing of terrorism facing them. Assessing this risk is, therefore, one of the most important steps in creating a robust anti-money laundering compliance program.

As money laundering risks increase, stronger controls are necessary. However, all categories of risk — whether low, medium or high — must be identified and mitigated by the application of controls, such as verification of customer identity, CDD policies, suspicious activity monitoring and checking list of people on whom sanctions have been applied or being applied. A risk-based approach should be flexible, effective and proportionate.

It is important to note that pursuant to section 3(2) of FIAML, dealers are required to take such measures that are necessary to ensure that their services are not being misused to commit a money laundering or the financing of terrorism offence. The penalty for such an offence is a fine not exceeding 10million rupees and penal servitude for a term not exceeding 20years. No dealer can reasonably be expected to detect all wrongdoing by clients, including money laundering. However, if any dealer develops systems and procedures to detect, monitor and report the riskier clients and transactions, he will reduce its chances of being misused by criminals.

There are three steps to establishing a risk-based approach: risk assessment, risk mitigation and risk monitoring. The following diagram depicts visually the three different steps in implementing a risk-based approach.
Risk Assessment

- Identify and rate the main ML/TF risks:
  - customers
  - products and services
  - business practices/delivery channels
  - geographical risk

Risk Mitigation

- Manage the business risks:
  - minimize and manage the risk
  - apply strategies, policies and procedures
  - put in place system and controls

Risk Monitoring

- Conduct on-going monitoring:
  - develop and carry out monitoring process
  - keep necessary records
  - report suspicious transactions
  - report to senior management
3.1.1 Risk Assessment

Dealers can assess money laundering and terrorist financing risks by using various categories. The application of risk categories provides a strategy for managing potential risks by enabling dealers to subject each customer to reasonable and proportionate risk assessment.

3.1.1.1 Criteria to determine Risk

The main risk categories are:

(a) Country or geographic risk;
(b) Customer and Counterparty risk;
(c) Product/services risk; and
(d) Business Practices/Delivery Channels.

The weight given to these risk categories (individually or in combination) in assessing the overall risk of potential money laundering may vary from one dealer to another, depending upon their respective circumstances. The categories however should be considered holistically and not in isolation.

The risk categories may be broken down into different levels of risks and they also help to determine the rigidity of your policies and procedures.

(a) Country or Geographic Risk

There is no unique definition of what consists a high-risk country or geographic location. However, there are several factors which can be considered when assessing whether a particular country or location presents higher risk. It is important to conduct such an assessment to ensure that dealers do not engage in transactions emanating from such countries or, if they do, that they have well established controls and procedures to mitigate the associated risk.

When it comes to the jewellery sector, some countries will present more serious AML/CFT concerns than others, and the risk level will vary depending on any of the elements of a transaction, including:\n
- Where the product is mined;
- Where the product is refined or finished;

The location of a seller or purchaser;

The location of the delivery of the product; and

The location of funds being used in the transaction.

In line with FATF guidance, the following factors should be considered by dealers when making an assessment of the country/geographical risk in relation to proposed transaction in diamonds, jewels or precious metals:

- For rough diamonds, whether a producing or trading country participates in the Kimberley Process.6

- Whether there is known mining or substantial trading of the transaction product – diamonds, jewels or precious metals - in a transaction source country.

- Whether a country would be an anticipated source of large stocks of existing diamonds, jewels or precious metals, based upon national wealth, trading practices and culture (centres of stone or jewel trading, such as Antwerp, Belgium) or unanticipated (large amounts of old gold jewellery in poor developing countries). In relation to this factor, consideration must be given to the cultural and economic significance of gold and silver in developing countries.

- The level of government oversight of business and labour in mining and/or trading areas.

- The extent to which cash is used in a country.

- The level of regulation of the activity.

- Whether informal banking systems operate in a country, e.g. hawalas operate in many developing countries.

- Whether designated terrorist organisations or criminal organisations operate within a country, especially in small and artisan mining areas.

- Whether there is ready access from a country to nearby competitive markets or processing operations, e.g. gold mined in Africa is more frequently refined in South Africa, the Middle East or Europe rather than in the United States, and a proposal to refine African gold in the United States would be unusual and higher risk.

6https://www.kimberleyprocess.com/. Mauritius is a participating country in this process.
Whether, based on credible sources, appropriate AML/CFT laws, regulations and other measures are applied and enforced in a country. Dealers may find it useful to consult the lists published by the FATF of those jurisdictions that have strategic deficiencies in their AML/CFT systems at the following link: https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/?hf=10&b=0&s=desc(fatf_releasedate). Information published by the Egmont group of FIUs may also assist. Dealers may also refer to any guidance issued by the IMF and any relevant national government bodies as well as nongovernmental organizations.

The level of enforcement of laws addressing corruption or other significant organized criminal activity.

Whether sanctions, embargoes or similar measures have been directed against the country.

(b) Customer and Counterparty Risk

i. Retail Customer Risk

The purchase of jewellery, precious metals or stones can be a very personal and emotional matter. It is widely accepted that these items are usually bought as gifts and in many cultures, occupy a significant place in weddings or other family events. Consequently, there will not, in general be a business purpose for such purchases. However, from an AML/CFT perspective, dealers must be conscious that not all purchases can simply be classified as emotional and therefore automatically legitimate. Higher risk may be observed at the retail level when the following factors are present (this is not an exhaustive, but an indicative list):

- **Use of cash.** It should be recognized, however, that many persons desire anonymity in jewellery purchases for purely personal reasons, or at least the absence of paper records, with no connection to money laundering or terrorist financing.

- **Payment by or delivery to third parties.** In these cases, dealers should nonetheless be aware that not all transactions involving third parties are suspicious since it is not uncommon for members of a family to select jewellery and for another member of the same family or any other close person to make the payment and have the product delivered.

- **Structuring.** Instances where a purchaser is making several purchases of lesser value deliberately.
ii. Business Counterparty Risk

There are many different stages and transactions and counterparties involved in the precious stones and precious metals businesses. Dealers may buy from or sell to other counterparties who also work in their precious metals or precious stones businesses, or sell to the public through retail sales (which may often be anonymous). Dealers will need to consider the risks associated with each stage at which they participate.

Higher risk counterparties (Example for Wholesalers)

- Lacks knowledge or understanding of the industry that he intends to deal in;
- Has no business premises or required equipment and financial resources necessary for the proposed business;
- Is unfamiliar with the business practices of the industry and the common financial terms and conditions;
- Proposes a transaction that makes no sense, or that is excessive, given the circumstances, in amount, or quality, or potential profit;
- Has significant and unexplained geographic distance from the dealer in precious metals or dealer in precious stones;
- Makes frequent and unexplained changes in bank accounts, especially among banks in other countries;
- Involves third parties in transactions, either as payers or recipients of payment or product, without apparent legitimate business purpose;
- Refuses to identify beneficial owners or controlling interests, where this would be commercially expected;
- Seeks anonymity by conducting ordinary business through accountants, lawyers, or other intermediaries, see the paragraph above;
- Prefers to deal non face to face;
- Uses cash in its transactions with the dealer in precious metals or dealer in precious stones, or with his own counterparties in a nonstandard manner;

- Uses money services businesses or other non-bank financial institutions for no apparent legitimate business purpose;

- Is a politically exposed person (PEP);

- Persons whose assets have been frozen under section 45 of the Dangerous Drugs Act or whose assets have been temporarily or permanently confiscated under the Asset Recovery Act; and

- Persons who appear on the UN Sanctions list or any domestic terrorist list pursuant to the UN Sanctions Act.

(c) **Product/Services Risk**

An overall risk assessment should also include a determination of the potential risks presented by products and services offered by a dealer in precious metals or a dealer in precious stones. The following factors may be considered when making such an assessment:

i. **Products**

While all precious metals and stones can potentially be used for money laundering and terrorist financing, level of risk will depend on the value of the item. Unless transactions involve very large quantities, lower value products are likely to carry less risk than higher value products. However, dealers must be conscious of the fact that value can also fluctuate dependent upon supply and demand. Relative values of some materials can vary dramatically between different countries, and over time.

The physical characteristics of the products offered must also be considered. Products that are can be transported or moved easily and which are unlikely to draw the attention of law enforcement are at greater risk of being used in cross border money laundering.

Finally, the risk of dealing in stolen or fraudulent products must be taken into account, given that jewellery theft has been identified as the main predicate offence associated with the sector in the NRA. Dealers must therefore be aware of the risks of trading in stolen products and of being offered
stolen jewellery. In addition to stolen goods, dealers should be alert to the fact that fraudulent goods may also be offered to them. Typically, this could involve 14 karat gold being represented as 18 karat. The risk associated with this possibility must also be taken into consideration. Buyers of second hand jewellery should be particularly conscious of this risk.

ii. Services

Along with the risk associated with the products being offered, dealers must also assess the risks associated with the services that they offer. Depending on the type of service being offered the risks may vary. For example, while some dealers may only be operating a retail business selling jewellery or stones, others may be involved in the cutting and polishing business where the risks might be different. Or if services are offered non face to face, for example services which are offered over the internet or telephone, the dealer will need to be aware of the risks which are connected to such services.

iii. Market Characteristics

It is also helpful to bear in mind the following broad principles which may lower the risk levels of particular transactions:

- **Limited resale opportunities** – limited resale opportunities are likely to be unattractive to money launderers.

- **Size of market** – a small market is likely to make it more difficult for a money launderer to structure transactions, to layer multiple transactions (to create distance between the seller and the ultimate purchaser), and to conduct anonymous transactions, and will thus be less attractive to money launderers.

- **Degree of expertise required** – if specialized expertise is required for transactions, risk of use of such transactions by money launderers may be lower.

- **Degree of market regulation** – if a market is regulated, depending upon the degree of regulation, transactions in that market may be lower risk.

- **Transaction costs** – money laundering and terrorist financing can involve multiple
transactions, with criminals first placing illegal assets within a legitimate product, as anonymously as possible, then layering those assets through intermediate transactions, and then removing them at a different time and place. Therefore transactions involving high value product and low transaction costs may be particularly attractive to money launderers and terrorist financiers. For example, a purchase of pure gold coins, and subsequent sale of those coins at another location, will quickly return most of the original purchase price.

iv. Financing Methods

The method of payment used affects the risk of money laundering and terrorist financing taking place. The risks are likely to be reduced if transactions take place through the mainstream banking system. Conversely, the risk may increase in the following situations:

- Cash, especially in large amounts, can be a warning sign, especially if the use of cash is anonymous or intentionally hides an identity, e.g. the true purchaser funds the transaction by giving cash to a third party, who then becomes the nominal and identified purchaser.

- Payments or delivery of product to or from third party accounts, e.g. accounts in the names of persons other than approved counterparties.

- Payments to or from accounts at financial institutions that are unrelated to a transaction or approved counterparties, such as banks located in countries other than the location of the counterparty or transaction.

- Non-bank financial mechanisms such as currency exchange businesses or money remitters.

(d) Business Practices/Delivery Channels

Dealers should also consider the channels used to deliver their products or services. In today’s economy and global market, many delivery channels do not bring the client into direct face-to-face contact with the reporting entity (for example, Internet, telephone or mail), and are accessible 24 hours a day, 7 days a week, from almost anywhere. The remoteness of some of these distribution channels can also be used to obscure the true identity of a client or beneficial owners and can therefore pose higher risks. The examination of business practices and delivery channels should also include conducting a risk assessment of any new technologies (eg. Internet based services)
that you are planning to implement. The risk assessment should be conducted prior to the new technology being implemented.

3.1.1.2 Risk Assessment Tool

A risk assessment tool at Annex 1 provides an example, for use by dealers, to facilitate the assessment of the above factors. However, a dealer's risk assessment has to be appropriate for their specific business needs which means that it may have to be more detailed than the checklist provided. Dealers can customize the checklist or can use a different method or another tool.

3.1.2 Risk Mitigation

The second component of a risk-based approach is risk mitigation. Risk mitigation is about implementing measures to limit the potential money laundering and terrorist financing risks the reporting entity has identified while staying within its risk tolerance level. Pursuant to section 17A of FIAMLA, dealers must establish policies, controls and procedures to mitigate and manage the ML/TF risks that they have identified as part of their assessment.

As part of its internal controls, when the risk assessment determines that risks are higher for ML or TF, the reporting entity has to develop written risk mitigation strategies (policies and procedures designed to mitigate high risk) and apply them for high risk situations.

It is important that the risk mitigation strategies are developed by the dealer for higher risk situations and that these mitigation strategies are documented. This allows the risk mitigation strategies to be shared with management and employees. Furthermore, the application of the mitigation strategies should be recorded to demonstrate that mitigation measures have been applied. Strong senior management leadership and engagement in AML/CFT is an important aspect of the application of the risk-based approach. Senior management should approve the risk mitigations strategies and ensure that they are reviewed every time the risk assessment is updated.

The development of a robust AML/CFT program is thus a crucial component of risk mitigation.

Risk mitigation strategies that can be applied have been identified at Annex 1.A.
3.1.3 Risk Monitoring

In addition to risk assessment and risk mitigation activities, a risk-based approach also requires dealers to take measures to conduct on-going monitoring of financial transactions when there is a business relationship. The level of monitoring should be adapted according the ML/TF risks as outlined in the entity’s risk assessment. The purpose of on-going monitoring activities is to help detect suspicious transactions. The dealer’s policies, controls and procedures have to determine what kind of monitoring is done for particular high-risk situations, including how to detect suspicious transactions. The policies, controls and procedures should also describe when monitoring is done (its frequency), how it is reviewed, and how it will be consistently applied.
4. Internal Controls

4.1 AML/CFT Program

An AML/CFT program is required to identify, mitigate and manage the risk of the products or services being offered by the dealer that could facilitate money laundering or terrorism financing. Through an AML/CFT program, the dealer is able to set out how it is going to implement its AML/CFT obligations.

As previously mentioned, AML/CFT programs should be risk-based. This means that dealers must develop their own program, tailored to their situation to mitigate money laundering and terrorism financing risks. This approach recognizes that not all aspects of an institution’s business present the same level of risks. The reporting person is in the best position to assess the risk of its clients, products and services and to allocate resources to counter the identified high-risk areas.

Although not exhaustive, the list below provides the basics of an AML/CFT program:

- Appointment of key officers
- Policies and Procedures
- Training
- Audit and Review

As mentioned at the start of this chapter, having an AML/CFT program enables the dealer to have a clear approach on how he is going to fulfill his AML/CFT obligations. These obligations are the following and are discussed in detail at Chapter 5 and Chapter 6 of these guidelines:

- Customer Due Diligence (CDD)
- Record Keeping
- Enhanced Due Diligence (EDD)
- Politically Exposed Persons (PEPs)
- Ongoing Monitoring
- Suspicious Transaction Reporting
- Training
- Terrorism Financing Obligations

Annex 2 provides a template to assist agents in the development of internal policies, procedures and controls.
4.1.1 **Appointment of Key Officers**

Subject to the size and nature of their business, Dealers, are required to appoint both a compliance officer and a Money Laundering Reporting Officer (MLRO) as part of their internal procedures and controls.

**4.1.1.1 The Compliance Officer**

The compliance officer (CO), who must be part of senior management is responsible for ensuring that the dealer is complying with its AML/CFT obligations.

The dealer must ensure that the CO:

(a) has timely and unrestricted access to the records of the dealer;

(b) has sufficient resources to perform his or her duties;

(c) has the full co-operation of the dealer’s staff;

(d) is fully aware of his or her obligations and those of the dealer; and

(e) reports directly to, and has regular contact with, the Board (where applicable) so as to enable the Board to satisfy itself that all statutory obligations and provisions in FIAMLA and the Regulations issued thereunder, are being met and that the dealer is taking sufficiently robust measures to protect itself against the potential risk of being used for ML and TF. Where there is no Board, the CO must report directly to the business owner or to any other senior officer appointed by the owner.

In accordance with Regulation22 (3) of the FIAML Regulations 2018, the functions of the CO include:

(a) ensuring continued compliance with the requirements of the FIAMLA and FIAML Regulations 2018 subject to the ongoing oversight of the Board of the dealer where applicable and senior management;
(b) undertaking day-to-day oversight of the program for combatting money laundering and terrorism financing;

c) regular reporting, including reporting of non-compliance, to the Board where applicable and senior management; and

d) contributing to designing, implementing and maintaining internal compliance manuals, policies, procedures and systems for combatting money laundering and terrorism financing.

For the avoidance of doubt, the same individual can be appointed to the positions of Money Laundering Reporting Officer ("MLRO") and CO, provided the dealer considers this appropriate with regard to the respective demands of the two roles and whether the individual has sufficient time and resources to fulfil both roles effectively.

**4.1.1.2 The Money Laundering Reporting Officer**

In accordance with Regulation 26(1) of FIAML Regulations 2018, the dealer shall appoint a MLRO to whom an internal report shall be made of any information or other matter which comes to the attention of any person handling a transaction and which, in the opinion of the person gives rise to knowledge or reasonable suspicion that another person is engaged in money laundering or the financing of terrorism. The MLRO must be sufficiently senior within the organization and must have the technical skills required to make an assessment of internal reports prior to determining whether an STR should be filed with the FIU.

There should be clear reporting lines internally, to ensure that all employees including directors or partners, know what the process is to report any suspicion that they may have internally to the MLRO. Records must be kept by the dealer of both internal and external disclosures.

Where due to its size or the nature of its business a dealer cannot appoint an MLRO, it must nevertheless have documented policies and procedures in place to ensure that it is complying with the FIAML and the 2018 Regulations. In these instances, the STR is filed by the dealer with the FIU directly.
4.1.2 Policies and Procedures

Dealers should have in place adequate policies, controls and procedures (PCPs) that promote high ethical and professional standards and prevent their business from being misused by criminals. These policies, procedures and internal controls should be efficiently introduced and maintained and each dealer should be aware of his responsibilities. PCPs should clearly document the steps which the dealer intends to follow in the implementation of each element of its AML/CFT Program. The dealer must for example have policies on employee screening and procedures detailing how it will meet the expectation set out in its policy.

All these PCPs must be widely publicized across the dealer’s business and all its employees must be made aware of their role and existence. They should also be easily accessible across the business.

4.1.3 Employment Screening and Training

4.1.3.1 Employment Screening

Dealers are required, under Regulation 22(1)(b) of FIAML Regulations 2018, to implement programmes for screening procedures so that high standards are maintained when hiring employees.

In light of the above, significance may be given to:

- Obtaining and confirming proper references at the time of recruitment;
- Requesting information from the member of staff with regard to any regulatory action taken against him; and
- Requesting information from the member of staff pertaining to any criminal convictions and the provision of a check of his criminal record (for instance, requiring a Certificate of Character).

4.1.3.2 Employee Training

Regulation 22(1)(c) of FIAML Regulations 2018 states that programmes against money laundering and terrorism financing should be in place to include ongoing training programme for the directors, officers and employees of the dealer, to maintain awareness of the laws and regulations relating to money laundering and terrorism financing to:

(i) assist them in recognizing transactions and actions that may be linked to money laundering or
terrorism financing; and

(ii) instruct them in the procedures to be followed where any links have been identified under subparagraph (i).

A training program should be designed to train the appropriate personnel on a regular basis. A successful training program not only should meet the standards set out in laws (i.e. FIAMLA Act 2002) but should also satisfy internal policies and procedures in place. For the purpose of this “Guidelines”, training includes not only formal training courses, but also communications that serves to educate and inform employees such as e-mails, newsletters, periodic team meetings and anything else that facilitates sharing of information.

Topics to be taught in the training program vary according to target audience and services being offered but several basic matters should be factored into the program:

- Policies and Procedures in place to prevent money laundering and financing of terrorism for instance identification, record-keeping, the recognition and reporting of suspicious transactions;
- Legal Requirements under relevant AML/CFT legislations and the statutory obligations under these laws;
- Understanding ML/TF risk of the sector and of their business;
- Penalties for anti-money laundering violations;
- How to react when facing a suspicious client or transaction;
- Duties and accountabilities of employees; and
- New developments together with information on current money laundering and financing of terrorism techniques, methods and trends.

Lastly, it would be advisable for dealers to keep a record of all anti-money laundering and combating the financing of terrorism training delivered to their employees.
4.1.4 Auditing the AML/CFT Program

Putting in place an AML/CFT Program is not sufficient; the program must be monitored and evaluated. The dealer should assess their anti-money laundering and combating the financing of terrorism programs at a minimum every two years to ensure their effectiveness and to look for new risk factors. The audit program should address issues such as (i) the adequacy of its ML/TF risk assessment, (ii) the adequacy of CDD policies, procedures and processes, and whether they comply with internal requirements, (iii) the adequacy of its risk-based approach in relation to the services offered clients and geographic locations, (iv) the training adequacy, including its comprehensiveness, accuracy of materials, training schedule, (v) compliance with applicable laws, (vi) the system's ability to identify unusual activity, (vii) the adequacy of recordkeeping and (viii) the review of its Suspicious Transaction Reporting (STR) systems, which should include an evaluation of the research and referral of unusual transaction among others.

The audit can be conducted by an internal or external auditor. If the reporting entity does not have an auditor, it can conduct a self-review. The self-review should be conducted by an individual who is independent of the compliance-monitoring functions and should not be conducted by the compliance officer. This could be an employee or an outside consultant. For sole proprietorships, the review can be conducted by the sole proprietor directly.

The objective of a self-review is similar to the objectives of a review conducted by internal or external auditors. It should address whether policies and procedures are in place and are being adhered to, and whether procedures and practices comply with legislative and regulatory requirements.

The results of the audit should be documented and presented either to the Board of Directors (if applicable) or to senior management. The recommended changes should be implemented no later than a month following the completion of the audit.
5. Preventive Measures

Once a dealer has put in place its AML/CFT Program, it can then implement its obligations under the FIAMLA, FIAML Regulations and the UN Sanctions Act. These are discussed below.

5.1 Customer Due Diligence: Identification and Verification Procedures

Both the FIAMLA and the FIAML Regulations make provision for CDD and KYC obligations and these apply to dealers as well.

In line with section 17C of FIAMLA, dealers need to identify and verify the true identity of the customer that they are conducting a transaction with. The identity of a customer must be established and verified using independent source documents, data or information. All CDD information collected must be kept up to date by the dealer. Additionally, CDD information must be verified against independent and reliable sources.

In case of corporate bodies, the company’s ultimate beneficial owner must be ascertained (see further below for more information on beneficial ownership) by obtaining information on their identity on the basis of documents, data or information obtained from a reliable and independent source and verifying the accuracy of the information obtained. The beneficial owner is the natural person who owns or controls the legal person or legal arrangement.

**Timing of CDD**

Identification and verification measures need to be carried out:
- When establishing a business relationship with a customer
- When dealing with a one-off customer or counterparty and the transaction concerned is equal to or above 500,000 rupees whether conducted as a single transaction or several transactions that appear to be linked;
- Where there is a suspicion of money laundering or financing of terrorism; and
- Where there are doubts concerning the veracity of previous customer/counterparty
identification information.

5.1.1 Natural Persons (i.e. Individuals)

(a) Face to Face transactions

Regulation 4 of the FIAML Regulations requires that the dealer shall obtain from and verify a customer who is a natural person the following information:

a. the full legal and any other names, including, marital name, former legal name or alias;
b. the date and place of birth;
c. the nationality;
d. the current and permanent address; and
e. such other information as may be specified by a relevant supervisory authority or regulatory body.

Identification and Verification Methods for Natural Persons

<table>
<thead>
<tr>
<th>Data to be collected</th>
<th>Verification Methods</th>
</tr>
</thead>
</table>
| 1. Full legal and any other names, including, marital name, former legal name or alias | • Current Valid National Identity Card  
• Current Valid Passport  
• Current valid driving licence- where the dealer is satisfied that the driving licensing authority carries out a check on the holder’s identity before issuing the licence. |
| 2. Date of birth | In each case, the document must incorporate a photographic evidence of identity. |
| 3. Gender | Where the legal person with which the natural person is associated is low or standard risk, then the method of verification for each required piece of data will normally suffice and can be one of the above methods. |
| 4. Place of birth | However, where the legal person is high risk, or where a high-risk rating would otherwise be attached to the individual principal, then the methods of verification will depend on the riskiness of the relationship and more than one method will be necessary |
| 5. Nationality | For self-employed, any of the sources below should be used:  
■ Trade Licence  
■ Business Registration Card |
| 6. Occupation and Name of Employer (if self-employed, the nature of the self-employment) | Any of the identity sources listed below:  
■ a recent utility bill issued to the individual by name;  
■ a recent bank or credit card statement; or  
■ a recent reference or letter of introduction from (i) a legal professional that is regulated in Mauritius; (ii) a regulated financial services business which |
(b) Non-Face-to-Face Transactions

It is most vital that the procedures adopted to verify identity of clients for non-face-to-face transaction is at least as robust as those for face-to-face verification. Accordingly, in accepting transactions from non-face-to-face clients, dealers should apply uniformly effective customer identification procedures as for those mentioned above and other specific and appropriate measures to mitigate the higher risk posed by non-face-to-face verification of clients.

In addition, for non-residents requiring services from abroad, details such as true name, current permanent address, mailing address, telephone and fax number, date and place of birth, nationality, occupation and name of employer (if self-employed, the nature of the self-employment), signature/signatures, authority to obtain any data provided.

Documents provided should be duly certified as a true copy by a lawyer, accountant or other professional person who clearly adds to the copy (by means of a stamp or otherwise) his name, address and profession to aid tracing of the certifier if necessary and which the dealer believes in good faith to be acceptable to it for the purposes of certifying.

5.1.2 Legal Persons and Legal Arrangements

Legal persons refers to any entities other than natural persons that can establish a permanent customer relationship with a reporting entity including a dealer or otherwise own property. In Mauritius, a legal person includes a company, a foundation, an association and a limited liability partnership. Legal arrangements, on the other hand, refers to express trusts or other similar legal arrangements. Examples of other similar arrangements (for AML/CFT purposes) include fiducie.
Regulations 5, 6 and 7 of the FIAML Regulations 2018 lay down specific requirements where an applicant is a legal person or a legal arrangement.

(a) Legal persons (For example: Companies)

Dealers must, in relation companies, understand and document the nature of the company’s business as well as the ownership and control structure. The following documents must be obtained to identify and verify the customer's identity:

i. The name, legal form and proof of existence of the company;
ii. Powers that regulate and bind the customer;
iii. The names of persons having senior management positions; and
iv. The address of the registered office or principal place of business.

### Identification and Verification Methods for Legal Persons

<table>
<thead>
<tr>
<th>Person to be identified</th>
<th>Data to be identified</th>
<th>Verification Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>Underlying persons who are individuals.</td>
<td>As per the requirements for natural person</td>
<td>▪ As per the requirements for natural person</td>
</tr>
<tr>
<td></td>
<td>Dealers should collect identification data in relation to the following: 1. Directors 2. Beneficial Owner(s) 3. Significant Shareholders and 4. Authorised signatories. In the absence of an authorised signatory, the identity of the relevant person who is the senior managing official. Senior managing official means an individual who makes, or participates in making, decisions that affect the whole, or a substantial part, of the business of a customer or who has the capacity to affect significantly the financial standing of a client.</td>
<td>▪ Where the legal person with which the underlying person is associated is low or standard risk, then the method of verification for each required piece of data will normally suffice and can be one of the above methods. ▪ However, where the legal person is high risk, or where a high-risk rating would otherwise be attached to the individual principal, then the methods of verification will depend on the riskiness of the relationship and more than one method will be necessary</td>
</tr>
<tr>
<td>1. Private companies</td>
<td>1. Legal status of body 2. Legal name of body 3. Any trading names</td>
<td>▪ Certificate of incorporation (or other appropriate certificate of registration or licensing);</td>
</tr>
<tr>
<td>2. Partnerships</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Sociétés</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------</td>
<td>----------------------</td>
<td></td>
</tr>
<tr>
<td>5. Other legal persons</td>
<td>5. Date and country of incorporation/registration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6. Official identification number (for example, company number)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>7. Registered office address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>8. Mailing address (if different)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>9. Principal place of business / operations (if different)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10. Any other data which the dealer consider to be reasonably necessary for the purposes of establishing the true identity of the legal person.</td>
<td></td>
</tr>
</tbody>
</table>

- Memorandum and Articles of Association (or equivalent);
- Company registry search, including confirmation that the person is not in the process of being dissolved, struck off, wound up or terminated;
- Latest audited financial statements or equivalent;
- Annual report or equivalent;
- Personal visit to principal place of business;
- Partnership deed or equivalent;
- Charter of Foundation;
- Acte de société;
- Certificate of good standing from a relevant national body;
- Reputable and satisfactory third-party data, such as a business information service
- Any other source of information that to verify that the document submitted is genuine.

(b) Legal Arrangements (For example: Trusts)

In the case of trusts, certified extracts of the original trust deed or probate copy of a will creating the trust, documentary evidence pertaining to the appointment of the current trustees and the nature and purpose of the trust. Additionally, the identity of the settlor, beneficiaries or class of beneficiaries and where applicable the protector or enforcer and any other natural person exercising ultimate effective control over the trust must be established and verified.

In the case of other legal arrangements, the dealer must identify and verify through reasonable means the identity of the persons in equivalent or similar positions to those described for trusts above.
<table>
<thead>
<tr>
<th>Person/ arrangement to be identified</th>
<th>Data to be identified</th>
<th>Verification Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>Underlying persons who are individuals.</td>
<td>As per the requirements for natural person</td>
<td>▪ As per the requirements for natural person</td>
</tr>
<tr>
<td>Underlying principals who are legal persons</td>
<td>As per the requirements for legal persons above</td>
<td>▪ As per the requirements for legal persons above</td>
</tr>
</tbody>
</table>
| Legal arrangement | 1. Legal status of arrangement (including date of establishment)  
2. Legal name of arrangement (if applicable)  
3. Trading or other given name(s) of arrangement (if applicable)  
4. Nature of business  
5. Any official registration or identifying number (if applicable)  
6. Registered office address (if applicable)  
7. Mailing address (if different)  
8. Principal place of business/operations (if different)  
9. Any other data which the dealer considers to be reasonably necessary for the purposes of establishing the true identity of the legal arrangement. | ▪ Trust deed or equivalent instrument  
▪ Official certificate of registration (if applicable)  
▪ Where the above proves insufficient, any other document or other source of information on which it is reasonable to place reliance in all the circumstances. |

Dealers must seek and obtain assurances from the trustee/s (or controlling individual/s) that all of the data requested by the Dealer under the above process has been provided, and that the individual(s) will notify the Dealer in the event of any subsequent changes.

Where identification information relating to a legal arrangement is not available from a public source, a Dealer will be dependent on the information that is provided by the legal arrangement (usually through its controlling individuals, such as trustees). Dealers should accordingly treat such information with care and in any event in accordance with the legal arrangement risk assessment.
5.1.3 Establishing and Verifying Beneficial Ownership

Section 17E(3) of the FIAML Act defines a ‘beneficial owner’ as a natural person:

i. Who ultimately owns or controls a customer;

ii. On whose behalf a transaction is being conducted;

iii. Includes those natural persons who exercise ultimate control over a legal person or arrangement; and

iv. Such other persons as may be prescribed.

In line with Regulation 6 of the FIAML Regulations, Dealers must identify and take reasonable measures to verify the identity of the beneficial owners. This should be done by obtaining the following information:

a) The identity of the natural persons having an ultimate controlling ownership interest in the company;

b) In the event the requirements of paragraph (a) cannot be fully satisfied, or where no natural person has control through ownership interests, the identity of the natural person who exercises control through other means; and

c) Where no natural person has been identified in (a) or (b), the identity of the natural person holding a senior management position.

When gathering the above data, dealers must document the process as well as any difficulties encountered during. Further enquiries may be made for verification such as verifying with the Registrar of companies, that the company continues to exist and has not been, or is not in the process of being, dissolved, struck off, wound up or terminated, by conducting in cases of doubt a visit to the place of business of the company, to verify that the company exists for a legitimate trading or economic purpose.

5.1.4 Individuals acting on Behalf of Applicants for Business and Customers

There might be cases where customers (particularly those which are legal persons) will have one or more individuals authorised to act on their behalf in dealing with dealers. As already mentioned
previously, it is not uncommon for third parties to purchase jewellery, precious metals or stones on behalf of another.

Dealers must have in place appropriate policies, procedures and controls to ensure that they are able to identify and verify the identity of all persons purporting to act on behalf of customers, and to confirm the authority of such persons to act. Dealers must, in the case of individuals acting on behalf of customers, obtain identification data and verify that data, in line with guidelines provided above.

Where the dealer is unable to determine whether the customer is acting for a third party or not, it shall make a suspicious activity report pursuant to section 14 of the FIAMLA to the Financial Intelligence Unit.

5.1.5 Third Party Reliance

In order to rely on another regulated/supervised/monitored person to perform CDD measures in accordance with section 17D of the FIAMLA, dealers must also ensure that the requirements of Regulation 21 of the FIAML Regulations are fulfilled and that –

i. the necessary information required is obtained immediately;
ii. he is satisfied that copies of identification data and other relevant documentation related to CDD requirements shall be made available from the third party upon request without delay;
iii. he is satisfied that the party is regulated and supervised or monitored for the purposes of combating money laundering and terrorism financing and has measures in place for compliance with CDD and record keeping requirements in line with the FIAMLA and FIAML Regulations; and
iv. he shall not rely on a third party based in a high-risk country.

5.1.6 Inability to Establish Customer Identity

Where the dealer cannot obtain all the information required to establish the identity of the customer to its full satisfaction, he shall not commence the business relation or perform the transaction and shall file a suspicious transaction report with the FIU.

Moreover, if during the course of its business activities, the dealer has doubts about the veracity or adequacy of previously obtained client identification data, he must identify and verify the identity of
the customer and beneficial owner before conducting any further

5.2 Record Keeping

All dealers are required to keep records of all the transactions in which they are involved and of all customers. The following records must be kept:

a) Records relating to the identification of customers and beneficial owners (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents) as well as business correspondence for at least 7 years after the business relationship has ended.

b) Records concerning transactions, both domestic and international shall be kept for a period of 7 years after the completion of the transaction; and

c) Copies of all STRs filed with the FIU shall also be kept for a period of at least 7 years from the date the report was made.

5.3 Enhanced Due Diligence (EDD)

Regulation 12 of the FIAML Regulations 2018 provides that dealers shall implement internal controls and other procedures to combat money laundering and financing of terrorism, including EDD procedures with respect to high-risk persons, business relations and transactions and persons established in jurisdictions that do not have adequate systems in place to combat money laundering and financing of terrorism.

Where the ML/TF risks are identified to be higher, dealers shall take EDD measures to mitigate and manage those risks.

The EDD measures that may apply for higher risk relationships should include:

(a) requesting additional information on the customer and updating on a frequent basis the customer or the beneficial owner;

(b) obtaining additional information on the intended nature of the business relationship and the source of fund/wealth;

(c) obtaining information on the intended or performed transactions;
(d) obtaining the approval of senior management to commence or continue the business relationship;

(e) conducting close monitoring of the business relationship; and

(f) any other measures the dealer may undertake with relation to a high-risk relationship.

Where a dealer is unable to perform the required Enhanced CDD requirements, the latter shall terminate the business relationship and file a suspicious transaction report under section 14 of the FIAMLA. See below for EDD measures to applicable to Politically exposed Persons (PEPs). A list of enhanced due diligence measures can be found at Annex 1.a.

5.4 Simplified Due Diligence

In general, the full range of CDD measures should be applied by dealers. However, simplified CDD measures can be implemented in cases where lower risks have been identified. The simplified CDD measures have to be commensurate with the lower risk factors and in accordance with any guidelines issued by a regulatory body or supervisory authority.

Where a dealer determines that there is a low level of risk, he shall ensure that the low risk identified is consistent with the findings of the national risk assessment or any risk assessment of his supervisory authority or regulatory body, whichever is most recently issued. Importantly, simplified CDD shall not apply where, a dealer knows, suspects, or has reasonable grounds for knowing or suspecting that a customer is engaged in money laundering or terrorism financing or that the transaction being conducted by the customer is being carried out on behalf of another person engaged in money laundering or terrorist financing. The possibility of applying simplified CDD is not an exemption. It only allows for the application of reduced measures. The ultimate decision rests with the dealer and there may be instances, depending on the level of risk and all the known circumstances (a high-risk relationship e.g. PEP will be dealt with more caution rather than the routine CDD measures), where it is inappropriate to adopt these simplified measures. Under all circumstances, dealers must keep the client risk assessment up to date and review the appropriateness of CDD obtained even if simplified CDD measures are adopted. Dealers are required to keep the risk assessment and level of CDD requirements under review and the level of risk of the CDD measures should be consistent with the risk of the relationship. Where simplified CDD measures are adopted, dealers should apply a risk-based approach to determine whether to adopt the simplified CDD measures in a given situation and/or
continue with the simplified measures, although these customers’ accounts are still subject to transaction monitoring obligations.

5.5 Politically Exposed Persons (PEPs)

PEPs are individuals who are or who have been entrusted with prominent public functions foreign, domestic and international organisation PEP, as well as the close relatives and associates of such persons. Pursuant to the FIAML Regulations 2018, PEPs have been classified as “domestic PEPs,” “foreign peps” and “international organization PEPs” in the FIAML Regulations.

5.5.1 Types of PEPs

(a) Domestic PEPs

A domestic PEP means a natural person who is or has been entrusted domestically with prominent public functions in Mauritius and includes the Head of State and of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials and such other person or category of persons as may be specified by a supervisory authority or regulatory body after consultation with the National Committee.

Examples on who may be a PEP

- Heads of state
- Heads of government
- Ministers and deputy or assistant ministers
- Members of parliament or similar legislative bodies
- Members of governing bodies of political parties
- Members of supreme courts, or any judicial body whose decisions are not subject to further appeal, except in exceptional circumstances
- members of courts of auditors or of the boards of central banks
- ambassadors, charges d' affaires and high-ranking officers in the armed forces
- members of the administrative, management or supervisory bodies of state-owned enterprises
- directors, deputy directors and members of the board of equivalent function of an international organization
(b) Foreign PEPs

Foreign PEPs have the same definition as above insofar as they are entrusted with prominent public function by a foreign country.

(c) International Organization PEPs

An “international organization PEP” means a person who is or has been entrusted with a prominent function by an international organization and included members of senior management or individuals who have been entrusted with equivalent functions including directors, deputy directors and members of the board or equivalent functions and such other person or category of person as may be specified by a supervisory authority or regulatory body after consultation with the National Committee.

(d) Close Associates and Family members

As provided by regulation 15(5) FIAML Regulations, in addition to the primary PEPs listed above, a PEP also includes close associates and family members.

i. Close associates mean-
   - an individual who is closely connected to a PEP, either socially or professionally; and
   - any other person as may be specified by a supervisory authority or regulatory body after consultation with the National Committee.

ii. Family members mean-
   - an individual who is related to a PEP either directly through consanguinity, or through marriage or similar forms of partnership; and
   - any other person as may be specified by a supervisory authority or regulatory body after consultation with the National Committee.

5.5.2 PEPs and Due Diligence Measures

Business relationships with PEPs pose a greater than normal money laundering risk to dealers, by virtue of the possibility for them to have benefitted from proceeds of corruption, as well as the potential for them (due to their offices and connections) to conceal the proceeds of corruption or other crimes.

As such, dealers are required to have a clear policy in relation to transactions involving such persons.
Dealers must therefore establish appropriate risk management systems to determine whether the customer or beneficial owner is a PEP. Regulation 12 of the FIAML Regulations prescribe that when dealing with domestic or international organization PEPs, the following EDD measures must be applied in addition to the normal CDD measures applicable under the Regulations:

(a) reasonable measures must be taken to determine whether a customer or the beneficial owner is a PEP; and

(b) in cases when there is higher risk business relationship with a domestic PEP or an international organization PEP, adopt the measures listed below:

- obtain senior management approval before establishing or continuing, for existing customers, such business relationships;
- take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as PEPs; and
- conduct enhanced ongoing monitoring on that relationship

Additionally, dealers shall apply all the above measures to family members or close associates of all types of PEP.

5.6 Reporting Suspicious Transactions

Pursuant to Section 14 of FIAML, dealers are obliged to file suspicious transaction reports (STRs) as soon as they become aware of a suspicious transaction. An STR must be filed not later than 5 working days after the suspicion arose. Failure to report an STR or failure to reasonably become aware of a suspicious transactions are both offences under the FIAML.

The FIU has an approved form for the filing of STRs which in accordance with section 15 of the FIAML, is to be used for reporting suspicious transactions. A copy of the form is available on the website of the FIU on the link below:


Information on the manner in which a STR shall be reported is contained in the FIU's Guidance Note No. 3 which is also available on the FIU’s website.
5.6.1 Suspicious Transaction

Under the FIAMLA, a suspicious transaction is one which gives rise to a reasonable suspicion that it may involve -

(a) the laundering of money or the proceeds of any crime; or
(b) funds linked or related to, or to be used for, the financing of terrorism or proliferation financing or any other activities or transaction related to terrorism as specified in the Prevention of Terrorism Act or under any other enactment whether or not the funds represent the proceeds of crime

Additionally, suspicious transactions:

(c) are made in circumstances of unusual or unjustified complexity;
(d) appear to have no economic justification or lawful objective;
(e) are made by or on behalf of a person whose identity has not been established to the satisfaction of the person with whom the transaction is made; or
(f) gives rise to suspicion for any other reason.

A transaction includes:

(a) opening an account, issuing a passbook, renting a safe deposit box, entering into a fiduciary relationship or establishing any other business relationship, whether electronically or otherwise; and
(b) a proposed transaction or an attempted transaction.

Ongoing Monitoring

The ability to file an STR of good quality is heavily reliant on the robustness of the systems put in place by the dealer. In fact, dealers are required to scrutinize transactions undertaken throughout the course of a business relationship, including where necessary the source of funds to ensure that the transactions are consistent with his knowledge of the customer. As part of the monitoring of transactions, dealers must examine the background and purpose of each transaction especially where these are complex, unusually large or conducted in unusual patterns. Equally, they must pay attention to transactions that do not seem to have an apparent economic or lawful purpose.
5.6.2 Request for Information by the FIU

Under section 13(2) (a) and 13(2)(b) of FIAMLA, the Director of the FIU may request additional information from dealers who submitted the suspicious transaction report or from any other reporting person which is, or appears to be, involved in the transaction. Also, pursuant to section 13(3) of the FIAMLA, the Director of the FIU can request information from dealers, whenever the FIU becomes aware of information that may give rise to reasonable suspicion of ML/TF offences, or it has received a request from investigatory/ supervisory/ overseas FIU/government agencies. The information sought for under the above sections shall, as soon as practicable but not later than 15 days, be furnished to the FIU.

Also, in line with section 13(6) of the FIAMLA, the FIU may order dealers to inform it if a person has been their client, or has acted on behalf of their client; or whether a client of the dealer has acted for a person.

If dealers fail to supply any information requested by the FIU under section 13(2), 13(3) or 13(6) of FIAMLA, they commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years as provided for in section 19 and 32A of the FIAMLA. Furthermore, the falsification, concealment, destruction or disposal of any document or material which is likely to be relevant to a request under Section 13(2), (3) or (6) also consists of an offence under the FIAMLA.

5.6.3 Protection of Information

Confidentiality is a key success factor for the operations of an FIU. In this context, the FIU has put in place a proper Program Level Security and a System Level Security policies and procedures. Under the Program Level Security (based on protection afforded under the law), and in line with section 30(1) of the FIAMLA, the Director, every officer of the FIU, the Chairperson and members of the Board shall take an oath of confidentiality before they begin to perform their duties. They should maintain during and after their relationship with the FIU, the confidentiality of any matter relating to the relevant enactments. Section 30(2) of the FIAMLA further provides that no information from which an individual or body can be identified and which is acquired by the FIU in the course of carrying out its functions shall be disclosed except where disclosure appears to the FIU to be necessary to enable
it to carry out its functions, or in the interests of the prevention or detection of crime, or in connection with the discharge of any international obligation to which Mauritius is subject. More so, in view of preserving the confidentiality of information disseminated, at the time of disclosure of intelligence to recipients, the FIU imposes terms and conditions on the usage of such intelligence in line with section 30(2A) of FIAML. Any breach of this section shall be punishable by a fine not exceeding Rs1 million and to imprisonment for a term not exceeding 3 years. Additionally, under the Program Level Security, the FIU has adopted clear policies on recruitment and termination of employment of staff.

**5.6.4 Tipping Off**

After making a suspicious transaction report to the FIU, section 16(1) of FIAML prevents dealers and any of their officers from informing anyone, including the customer, about the contents of a suspicious transaction report or even discloses to him that he/she has made such a report or information has been supplied to the FIU pursuant to the request made under section 13(2), 13(3) or 13(6) of FIAML. It shall amount to an offence under the Act punishable by a fine not exceeding five million rupees and to imprisonment for a term not exceeding 10 year.

Reasonable enquiries of a customer, conducted in a discreet manner, regarding the background to a transaction or activity which has given rise to the suspicion is prudent practice, forms an integral part of CDD and on-going monitoring, and should not give rise to tipping off. If the employee suspects that CDD will tip off the client, the employee should stop conducting CDD and instead the dealer should immediately file an STR with the FIU.

**4.1.8.5 Registration with the FIU**

In line with section 14C of the FIAML, the dealer must register with the FIU, within such time, form and manner as may be prescribed. The Financial Intelligence and Anti Money Laundering (Registration of Reporting Persons) Regulations 2019 were made on 5th November 2019 to this effect. All dealers under the FIAML must register with the FIU in accordance with the time frames which shall be specified by the FIU. When the FIU specifies the time frame for the jewellery sector, it shall also issue guidance on how to register to assist each reporting person.

**5.8 Cash Prohibition**

Moreover, dealers shall not make or accept any payment in cash in excess of 500,000 rupees or an equivalent amount in foreign currency pursuant to section 5 of FIAML. Under FIAML, "cash" means
money in notes or coins of Mauritius or in any other currency; and it includes any cheque which is neither crossed nor made payable to order whether in Mauritian currency or in any other currency.
6. Terrorist Financing Offences

6.1 Introduction

Terrorist organizations require funds to plan and carry out attacks, train militants, pay their operatives and promote their ideologies. The Convention for the Suppression of the Financing of Terrorism Act and the Prevention of Terrorism Act criminalize the financing of the terrorism in Mauritius. Additionally, the UN Sanctions Act provides the legal framework for implementing targeted financial sanctions imposed by the United Nations Security Council.

6.2 Extension of Obligations

According to section 19H & K of the FIAMLA, a dealer falling under the purview of a regulatory body must ensure compliance with the UN Sanctions Act. Dealers should be aware that once a person has been designated domestically or listed by the UN, it is an offence to deal with the funds or other assets of such a person. It is also an offence to make funds or other assets available to a designated party or listed party. As soon as there is a designation or a listing, two prohibitions prevail under the UN Sanctions Act:

- A prohibition to deal with the funds or other assets of the designated or listed party under section 23; and
- A prohibition to make available funds or other assets to the designated or listed party under section 24.

The prohibitions to apply to all persons (including all dealers)

Under the UN Sanctions Act, there are also several reporting obligations which apply to dealers. These are set out below.

6.3 Reporting Obligations

Where any person holds, controls or has in his custody or possession any funds or other assets of a designated party or listed party, he/she shall immediately notify (section 23(4) UN Sanctions Act) the National Sanctions Secretariat of-

i. details of the funds or other assets against which action was taken against;

ii. the name and address of the designated party or listed party; and
iii. details of any attempted transaction involving the funds or other assets, including-

- the name and address of the sender
- the name and address of the intended recipient
- the purpose of the attempted transaction
- the origin of the funds or other assets
- where the funds or other assets were intended to be sent.

The reporting obligations continue under section 25 of the UN Sanctions Act which says that a reporting person shall immediately verify whether the details of the designated or listed party match with the particulars of any customer and if so, identify whether the customer owns any funds or other assets in Mauritius. A report has to be submitted to the National Sanctions Secretariat regardless of whether any funds or other assets were identified by the reporting person.

Contact details for the National Sanctions Secretariat:

**National Sanctions Secretariat**

Prime Minister’s Office (Home Affairs)
Fourth floor
New Government Centre
Port Louis

Phone Number: (+230) 201 1264 / 201 1366
Fax: (+230) 211 9272
Email: nssec@govmu.org

### 6.4 Reporting of Suspicious Information

Pursuant to section 39 of the UN Sanctions Act, any information related to a designated party or listed party which is known to the dealer should be submitted to the FIU in accordance with section 14 of the FIAMLA. For more information on how to file an STR please refer to Section 5.6 of this guideline.

### 6.5 Internal controls

Section 41 of the UN Sanctions Act states that a reporting person shall implement internal controls and other procedures to enable it to effectively comply with their obligations under this Act. As such, when a dealer designs his AML/CFT program, detailed in the previous section, he must also ensure that he incorporates policies and procedures to ensure that he is not engaging in any transactions with
designated or listed parties. Each of the building blocks of his AML/CFT program must also take into account the obligations under the UN Sanctions Act and the dealer must have systems which will allow him to screen customers against the lists of designated or listed parties maintained by the NSS on its website. Additionally, any dealer already registered with the FIU will also receive any changes to these lists as soon as these are made.
7. ML/TF Indicators for Dealers

There are a number of situations which may give rise to a suspicion that a transaction may involve money laundering. The list of situations given below is meant to assist dealers to detect/identify suspicious or unusual transactions in the conduct of their operations and business activities. It is not a prescriptive list of all possible transactions linked to money laundering or terrorism financing. Nor does it imply that the transactions listed below are necessarily linked to such activities. The role of dealers is to be familiar with these indicators, and exercise sound judgment based on their knowledge of the precious metals and stones industry, and where they identify any “suspicious or unusual transactions”, to know the proper action to take.

7.1 General Indicators

- Client indiscriminately purchases merchandise without regard for value, size, or color of precious stones.
- Purchases or sales that are unusual for client or supplier.
- Unusual payment methods, such as large amounts of cash, multiple or sequentially numbered money orders, traveler’s checks, or cashier’s cheques, or payment from third-parties.
- Attempts by client or supplier to maintain high degree of secrecy with respect to the transaction, such as request that normal business records not be kept.
- A client orders item, pays for them in cash, cancels the order and then receives a large refund.
- A client asking about the possibility of returning goods and obtaining a cheque (especially if the client requests that cheque be written to a third party).
- A client paying for high-priced jewellery or precious metal with cash only.
- A client not asking for a reduced price or negotiating over the list price, in circumstances where such practices are traditional or common.
- Purchase appears to be beyond the means of the client based on his stated or known occupation or income.
- Client may attempt to use a third party cheque or a third party credit card.
- Funds come from an offshore financial centre rather than a local bank.
- Large or frequent payments made in funds other than rupees.
- Transaction lacks a business purpose.
- Purchases or sales that are not in conformity with standard industry practice.
7.2 Indicators for Wholesalers

- The funds come from an offshore financial centre instead of a local bank.
- Over or under-invoicing, structured, complex, or multiple invoice requests, and high-dollar shipments that are over or underinsured.
- Unwillingness by a supplier to provide complete or accurate contact information, financial references or business affiliations.
- Counterpart presence, such as an affiliated store or branch or associate, in non-cooperative countries and territories or countries that are the subject of advisories issued by the Financial Action Task Force.
Annex 1. Risk Assessment Form for Dealers

Name of Dealer: _______________________________________________

The Financial Intelligence Anti-Money Laundering Act requires dealers to conduct a risk assessment of your exposure to money laundering and terrorism financing and apply corresponding mitigation and controls. This checklist is meant to assist you in meeting these obligations. This form is presented as an example only. You may choose to conduct your risk assessment using a different approach.

Instructions: When you answer yes to one of the questions, this situation or client is considered higher risk and a control measures to reduce the risk should be applied. For each higher risk client or situation a suggested control measure is proposed. You can adapt the control measures to correspond to your business (see Annex 1.A for a list of control measures).

The results of this risk assessment should be communicated to all owners, managers and employees in your business that deal with clients. The training should include a review of what is considered higher risk and the corresponding control measures. The date of the training should be documented. You should review your risk assessment every two years.
## Risk Assessment

### Higher risk clients and situations

<table>
<thead>
<tr>
<th>Yes Higher risk</th>
<th>No Moderate Risk</th>
<th>Suggested Control Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Clients</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are your clients foreigners?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you have clients who are politically exposed persons?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is your client a company, trust, foundation, partnership or other structure that makes it difficult to determine who is the beneficial owner (the natural person who owns or controls the funds or property)?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are your clients intermediaries (i.e. lawyers and accountants acting on behalf of clients)?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Has one of your clients been named in the media as being involved with criminal organizations or having committed a crime?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you have a client that is purchasing precious metals and stones that is not within his or her means based on his stated occupation or income?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do your clients that engage in activities that are consistent with the indicators identified for Suspicious Transactions? (See Guidance Note on AML/CFT Guidance on Suspicious Transaction Reports for suspicious transactions indicators and the indicators listed in this guideline).</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Suggested Control Measures

- Determine if individuals are politically exposed persons.\(^7\)
- Obtain additional information on source of funds or source of wealth.
- Obtain senior management approval to conduct the transaction.
- Obtain additional information on source of funds or source of wealth.
- Conduct enhanced on-going monitoring any future real estate transactions.
- Obtain name of natural person(s) behind company, trust or other legal arrangements.\(^8\)
- Obtain additional information on organizational structure.
- Obtain additional information on source of funds or source of wealth.
- Obtain name of person(s) on whose behalf the transaction is being conducted.
- Verify that the intermediary has the necessary documentation to act on behalf of the client.
- Obtain additional information on source of funds or source of wealth.
- Obtain additional information on source of funds or source of wealth.
- Obtain additional information on source of funds or source of wealth.
- Consider filing a Suspicious Transaction Report (STR).
- Obtain additional information on source of funds or source of wealth.

---

\(^7\)Pursuant to FIAMLA, you are required to ascertain whether all clients and beneficial owners are politically exposed persons. The mitigation measure is suggested here for emphasis.

\(^8\)For further information on how to comply with your beneficial ownership obligations please consult the Guideline on the Prevention of Money Laundering and Countering the Financing of Terrorism in the Real Estate Sector.
<table>
<thead>
<tr>
<th><strong>Products, services and transactions</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Do you undertake high value transactions?</td>
</tr>
<tr>
<td>▪ Pay special attention for unusual transaction and ML/TF indicators.</td>
</tr>
<tr>
<td>▪ Obtain additional information on source of funds or source of wealth.</td>
</tr>
<tr>
<td>Do you sell gold bars or loose diamonds?</td>
</tr>
<tr>
<td>▪ Pay special attention for unusual transaction and ML/TF indicators.</td>
</tr>
<tr>
<td>▪ Obtain additional information on source of funds or source of wealth.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Geographic Risk</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Are any of your clients or the source funds originate from countries subject to sanctions, embargoes or similar measures issued by Mauritius or International Organizations such as the United Nations (“UN”).</td>
</tr>
<tr>
<td>▪ Obtain senior management approval to proceed with the transaction.</td>
</tr>
<tr>
<td>▪ Ask for additional information, piece of identification to confirm the identity.</td>
</tr>
<tr>
<td>▪ Obtain additional information on source of funds or source of wealth.</td>
</tr>
<tr>
<td>Are any of your clients or the source funds originate from foreign jurisdictions known for high levels of financial secrecy or jurisdictions with low tax rates?</td>
</tr>
<tr>
<td>▪ Obtain senior management approval to proceed with the transaction.</td>
</tr>
<tr>
<td>▪ Ask for an additional piece of identification to confirm the identity.</td>
</tr>
<tr>
<td>▪ Obtain additional information on source of funds or source of wealth.</td>
</tr>
<tr>
<td>Are any of your clients or the source funds originate from foreign jurisdictions identified by the Financial Action Task Force (FATF) as having strategic deficiencies in the fight against money laundering or subject to an FATF statement?</td>
</tr>
<tr>
<td>▪ Obtain senior management approval to proceed with the transaction.</td>
</tr>
<tr>
<td>▪ Ask for an additional piece of identification to confirm the identity.</td>
</tr>
<tr>
<td>▪ Obtain additional information on source of funds or source of wealth.</td>
</tr>
<tr>
<td>Question</td>
</tr>
<tr>
<td>---</td>
</tr>
</tbody>
</table>
| Do any of your clients or the source funds originate from jurisdictions identified by credible sources (for example international organizations such as the UN, credible news reports) as providing funding or support for terrorist activities? | ▪ Obtain senior management approval to proceed with the transaction.  
▪ Ask for an additional piece of identification to confirm the identity.  
▪ Obtain additional information on source of funds or source of wealth.  
| Do any of your clients or the source funds originate from countries identified by credible sources as having significant levels of corruption, or other criminal activity? | ▪ Obtain senior management approval to proceed with the transaction.  
▪ Ask for an additional piece of identification to confirm the identity.  
▪ Obtain additional information on source of funds or source of wealth. |
| Are any of your clients or the source funds originate from a high level of financial secrecy? | ▪ Obtain senior management approval to proceed with the transaction.  
▪ Ask for an additional piece of identification to confirm the identity.  
▪ Obtain additional information on source of funds or source of wealth.  
| **Delivery Channel and Business Practices** | |
| Do you accept cash? | ▪ Confirm source of funds  
▪ Set limits to cash transaction amounts recognizing the 500,000 rupee cash prohibition outlined in the FIAMLA.  
▪ Request bank drafts instead of accepting large amounts of cash. |
| Do you conduct transactions where you do not meet the client? | ▪ Deliver comprehensive AML/CFT training to your employees specifically focused on client due diligence requirements  
▪ Ask for an additional piece of identification to confirm the identity.  
▪ Confirm the beneficial owner (the natural person who owns or controls the funds or property)  
▪ Confirm that any intermediary has the necessary documentation to act on behalf of the client.  
▪ Conduct periodic review of records to ensure that client due diligence requirements are adequately implemented |
| Do you have clients that are referred to you by a third party (such as a lawyer, accountant or other real estate agent)? | ▪ Conduct client due diligence measures directly.  
▪ Conduct periodic review of records to ensure that client due diligence requirements are respected by third party if you rely on them for due diligence measures. |
<p>| Do you have short-term or part-time employees? | ▪ Include AML/CFT obligations in job descriptions and performance reviews. |</p>
<table>
<thead>
<tr>
<th>Other risk factors: (list any additional factors)</th>
<th></th>
</tr>
</thead>
</table>

- Deliver comprehensive AML/CFT training for all employees

**Signature of the Dealer**

**Date**

**Date of employee training:**

__________________________________________
Annex 1.A - Examples of Risk Control Measures

1. Obtain senior management or compliance officer approval to proceed with the transaction.
2. Ask for an additional piece of identification to confirm the identity.
3. Obtain name of natural person(s) behind company, trust or other legal arrangement.
4. Monitor if client conducts additional real estate transactions.
5. Obtain information on source of funds or source of wealth of the client.
6. Deliver more frequent employee training.
7. Monitor AML/CFT legislative and regulatory changes.
8. Include AML/CFT obligations in job descriptions and performance reviews.
9. Set limits to cash transaction amounts (less than the 500,000 rupees prohibition).
10. Request bank drafts instead of accepting large amounts of cash.
11. Conduct transaction only in person.
12. Obtain appropriate additional information to understand the client’s business or circumstances.
13. Conduct transaction only in person.
14. Carrying out additional searches (e.g. internet searches using independent and open sources) to better inform the client risk profile (provided that the internal policies of accountants should enable them to disregard source documents, data or information, which is perceived to be unreliable).
15. Obtaining additional information and, as appropriate, substantiating documentation, on the intended nature of the business relationship.
16. Obtaining information on the source of funds and/or source of wealth of the client and clearly evidencing this through appropriate documentation obtained.
17. Obtaining information on the reasons for intended or performed transactions.
18. Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.
19. Requiring the first payment to be carried out through an account in the client’s name with a bank subject to similar CDD standards.
20. Enhanced CDD may also include lowering the threshold of ownership for beneficial ownership purposes, to ensure complete understanding of the control structure of the entity involved. It may also include looking further than simply holdings of equity shares, to understand the voting rights of each party who holds an interest in the entity.
NAME OF ENTITY

Risk Assessment and Risk mitigation (Section 17 of the Financial intelligence Anti-Money Laundering Act (FIAMLA))

Describe how you will comply with your risk assessment and risk mitigation obligations including:

- Identifying what clients and situations you have identified as higher risk (copy of the risk assessment should be attached)
- What mitigation and control measures you will be implementing to reduce the risk
- How you will document the risk of any new product or services
- How often you will update the risk assessment

See How to conduct a risk assessment in the precious metals and stones sector for additional guidance (Please refer to Annex 1).

Customer due diligence (CDD): (section 17C of the FIAMLA)

Describe how you will comply with CDD requirements including:

- When will you identify the buyer and seller of a transaction?
- What information will you collect when you identify a natural person?
- What information will you collect when you identify a legal persons and legal arrangements?
- What identification documents are acceptable?
- Only original documents will be acceptable
- How will you identify clients that are not physically present?
- What will you do if you cannot complete customer due diligence measures?

Record Keeping (Section 17F of FIAMLA)

Describe how you will comply with record keeping requirements including:
How long will you retain records related to transactions?
What records will you retain?
Where will records be retained?
How will you ensure that information can be provided in a timely manner to the Financial Intelligence Unit, the police and other competent authorities?
If you are using a third party to conduct customer due diligence measures:
  o How you will ensure that they are properly identifying clients?
  o How you will gain access to information in a timely fashion?

Enhanced due diligence (Regulation 12 of the Financial Intelligence Anti-Money Laundering Regulations (FIAMLR))

Describe how you will comply with enhanced due diligence requirements including:

  ▪ How you will apply enhanced due diligence measures to:
    o Persons or transactions involving a country identified as higher risk by FATF
    o Persons or transactions involving higher risk countries for ML, TF, corruption or subject to international ML/TF
    o Any other situation representing a higher risk of ML/TF based on your risk assessment
  ▪ What enhanced due diligence measures will be applied in those circumstances?

Politically Exposed Persons (Regulation 15 of the FIAMLR)

Describe how you will comply with enhanced due diligence requirements related to politically exposed persons including:

  ▪ What is a politically exposed person?
  ▪ How you will identify politically exposed persons?
  ▪ How you will seek approval from senior management?
  ▪ How you will take adequate measures to establish source of wealth and source of funds?
  ▪ How you will conduct enhanced ongoing monitoring?

Ongoing monitoring (Section 3 (e) of the FIAMLR)

Describe how you will comply with ongoing monitoring requirements including:

  ▪ How you will conduct ongoing monitoring for:
o Business relationships (typically after 2 transactions)
o Complex and unusual transactions
  o Unusual patterns of transactions which have no economic or lawful purpose?
  ▪ How you will record the findings?

---

**Suspicious transaction reporting (Section 15 of the FIAMLA)**

Describe how you will comply with suspicious transaction reporting requirements including:

▪ What is a suspicious transaction?
▪ How you and your employees/agents will identify suspicious transactions (should refer to ML/TF indicators)
▪ Who is your Money Laundering Reporting Officer?
▪ How employees/agents should raise suspicions to the reporting officer?
▪ Specify that you cannot communicate that an STR has been filed with the FIU

---

**Training (Regulation 22 (1) (c) of the FIAMLR)**

Describe how you will comply with training requirements including:

▪ How you will screen employees to ensure high standards before hiring
▪ How you will train employees/agents on:
  o How to identify a suspicious transaction?
  o What are the AML/CTF obligations?
  o How to implement your policies and procedures?

---

**Terrorist Financing Obligations (Regulation 22 (1) (c) of the FIAMLR)**

▪ Describe how you will comply with training requirements including:
  o How you will screen against UN Sanctions List?
  o How you will report to the National Sanctions Secretariat?
  o How you will report to the FIU?

---

**Policies and procedures (Section 22 (1) (c) of the FIAMLR)**

Describe the following regarding your policies and procedures:

▪ How you will communicate the policies and procedures to employees and staff as well as branches
and subsidiaries

- How you will reflect changes to AML/CTF legislative and regulatory requirements
- How often you will update your policies and procedures
CONTACT DETAILS

Financial Intelligence Unit
Compliance Division

10th Floor SICOM Tower
Ebene Cybercity
Republic of Mauritius
Telephone: (230) 454 1423
Fax: (230) 466 2431
Email: compliance@fiu mauritius.org