FINANCIAL INTELLIGENCE AUTHORITY

The Supervision Unit

Guidance to Reporting Entities on Applying a Risk Based Approach and Conducting ML/TF/PF Risk Assessments

March 2022

List of Acronyms

AML	Anti-Money Laundering
ATA	Anti-Terrorism Act
CFATF	Caribbean Financial Action Task Force
CFT	Countering Financing of Terrorism
CPF	Counter Proliferation Financing
FATF	Financial Action Task Force
FI	Financial Institutions
FIA	Financial Intelligence Authority
ML	Money Laundering
MLPA	Money Laundering Prevention Act
NRA	National Risk Assessment
OBA	Other Business Activities
OECD	Organisation for Economic Cooperation and Development
OFAC	Office of Foreign Assets Control
PEP	Politically Exposed Person
PF	Proliferation Financing
RBA	Risk Based Approach
SAR	Suspicious Transaction Report
TF	Terrorist Financing

Terms Used in This Guideline

- **Beneficial Owner** - means a natural person —
  - who ultimately owns or controls a company or legal arrangement;
  - who exercises ultimate effective control over a legal person or a legal arrangement, such as a senior manager or signatory; or
  - on whose behalf a transaction or activity is being conducted;

- **Emerging Risk** – means a risk that has never been identified before or an existing risk that has significantly increased.

- **Impact** – means the consequence or harm that ML, TF or PF 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

- **Inherent Risk** - means the risk of an event or circumstance that exists before you implement controls or mitigation measures

- **Likelihood** – the probability of a ML, TF or PF risk occurring

- **ML/TF/PF Risk** - means the likelihood of ML/TF/PF occurring and its impact (consequences). It is a combination of the chance that something may happen and the degree of damage or loss that may result.

- **ML/TF/PF Risk Factors** - means variables that, either on their own or in combination, may increase or decrease ML/TF risk.

- **Residual Risk** – the ML, TF, or PF risk remaining after taking into consideration risk mitigation measures and controls

- **Risk Appetite** – means the framework developed by the senior management and board of directors prescribing the type and level of risk that a reporting entity is prepared to accept. It specifies the boundaries that must be respected when pursuing the reporting entity's strategy.

- **Risk Based Approach –** means the identification, assessment, and understanding of the ML, TF and PF risk exposure, and the application of the appropriate mitigation measures commensurate with the level of risk.

- **Risk Profile -** means the overall characteristics of the ML/TF/PF risk associated with the subject of assessment or sector/sub-sector, including the type and level of risk

- **Politically Exposed Persons**

    - *Foreign PEPs* are individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.

    - *Domestic PEPs* are individuals who are or have been entrusted domestically with prominent public functions, e.g. Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.

    - *International PEPs* are individuals who are or have been entrusted with a prominent function by an international organisation such as senior management, directors, deputy directors and members of the board or equivalent functions.

- **Threat** – means 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, a threat could include criminals, terrorist groups and their facilitators, their funds, as well as past, present and future ML or TF activities.

- **Ultimately Own and Control** - means a direct or an indirect ownership or control of twenty-five percent or more of the shares, voting rights or ownership interest in a company or a legal arrangement.

- **Vulnerability** – means those things that can be exploited by the threat or that may support or facilitate its activities. In the ML/TF risk context, vulnerabilities include the factors that represent weaknesses in AML/CFT systems or controls or certain features of an entity. 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.

Table of Contents

1.0 Overview/Introduction 1
2.0 Scope of the Guidelines 1
3.0 Obligation to Conduct AML/CFT/CPF Risk Assessments 2
4.0 Frequency of Reviews and Updates 2
5.0 Responsibility for the Risk Assessment 2
6.0 The Risk Based Approach 2
7.0 The Risk Assessment Process 3
7.1 What is Risk? 3
7.2 What is Risk Management? 3
7.3 Which Risks must be Managed? 3
8.0 Identifying the ML/TF/PF Risks 5
8.1 Customer Risks 5
8.2 Product/Service Risks 5
8.3 Geographic Risks 6
8.4 Transaction and Delivery Channel Risks 7
8.5 Any Other Factors 7
9.0 Assessing and Categorising the Inherent ML/TF/PF Risks 7
9.1 Likelihood Scale 8
9.2 Impact Scale 8
9.3 Inherent Risk as a Function of Likelihood and Impact 9
10.0 Evaluating AML/CFT/CPF Internal Controls 10
10.1 Internal Control Factors 11
11.0 Determination of Residual Risk 11
12.0 Documentation of the ML/TF/PF Risk Assessment Results 12
13.0 Updating of the ML/TF/PF Risk Assessment 13
Appendix 1: Description of Risk Factors 14

1.0 Overview/Introduction

The power to issue guidelines are conferred onto the Financial Intelligence Authority (the Authority) by Section 6 (1) (f) of the Money Laundering (Prevention) Act, Cap 12.20 of the Laws of Saint Lucia (the MLPA). The purpose of these guidelines is to assist reporting entities in ensuring compliance with Section 16B of the Money Laundering (Prevention) (Amendment) Act No. 16 of 2021 (the MLPA Amendment Act), which requires all reporting entities to conduct risk assessments of its operations in relation to money laundering, terrorist financing and proliferation financing by identifying, assessing, and understanding its ML, TF and PF risks. In addition, the guidelines serve to provide a framework on how to conduct and document the AML/CFT/CPF risk assessment.

Subsequent to the conduct of the risk assessment reporting entities are required to take appropriate measures to mitigate the identified risks. The AML/CFT/CPF Compliance programme implemented by the reporting entity must reflect the identified risks. Thus, the extent to which a reporting entity understands its risks is a crucial element for the development and implementation of appropriate and adequate measures, which are commensurate to the nature and size of its business, for the proper management and mitigation of those risks.

The guidance provided in these guidelines will be subjected to ongoing reviews and will be updated as needed to reflect any new changes in the money laundering (ML), terrorist financing (TF), proliferation financing (PF) trends and patterns domestically and internationally which may pose a risk to the reporting entities.

2.0 Scope of the Guidelines

The guidelines are being issued to all reporting entities listed in Schedule 2, Parts A and B of the Money Laundering (Prevention) (Amendment) Act No. 16 of 2021, except licensed financial institutions which are licensed under the Banking Act, Cap. 12.01.

Following these guidelines is not mandatory. They reflect best practice internationally and implement the recommendations of the Financial Action Task Force (FATF). The FIA recognizes that reporting entities may have systems and procedures in place which, whilst not identical to those outlined in these Guidelines, nevertheless impose procedures, that are at least equal to if not higher than those contained in these Guidelines. Reporting entities are required to develop and implement effective ML/TF/PF risk assessment frameworks and establish AML/CFT/CPF Compliance Progammes.

3.0 Obligation to Conduct AML/CFT/CPF Risk Assessments

Pursuant to Section 16B of the Money Laundering (Prevention) (Amendment) Act No. 16 of 2021, every reporting entity is required to conduct risk assessments of its operations in relation to money laundering, terrorist financing and proliferation financing by identifying, assessing and understanding the ML, TF and PF risk posed by the following factors:

- existing or potential customers
- countries or geographic areas
- products, services, or transactions
- delivery channels for products, services, or transactions

When conducting the risk assessment, the reporting entity must, in line with Section 16B (2) (b) of the MLPA Amendment Act consider all relevant risk factors, including the risks identified by the country's national risk assessment (NRA), before determining the level of overall risk and the appropriate level and type of mitigation to be applied.

The reporting entity is required to document the outcome of the risk assessment, keep it up to date and develop appropriate mechanisms to provide risk assessment information to the FIA.

4.0 Frequency of Reviews and Updates

Risk is not static, and as such the risk assessment must be kept up to date and adjusted to reflect changing circumstances. The risks that are identified may change or evolve over time as they may be triggered by new products, new customers, new geographies, new threats to the operations, changes to the reporting entity's risk tolerance or regulatory changes.

5.0 Responsibility for the Risk Assessment

The ultimate responsibility for ensuring that the risk assessment is undertaken lies with the reporting entity's Board of Directors/Owners.

The reporting entity's Board of Directors/Owners should understand the nature and level of the risks that the reporting entity is exposed to and ensure that systems and processes exist to identify, assess, monitor, manage and mitigate ML/TF/PF risks by allocating appropriate resources and expertise to the development of the risk assessment.

6.0 The Risk Based Approach

Reporting entities should adopt a risk-based approach to their AML/CFT/CPF Compliance Programmes as it is an effective way to prevent or mitigate ML, TF and PF. The RBA

ensures that the AML, CFT and CPF measures applied by the entity are commensurate to the risks identified, thus allowing for the allocation of resources in the most efficient way. Thereby ensuring that higher risk areas receive more resources to manage and mitigate risk than lower risk areas.

The application of the RBA requires reporting entities to consider all the relevant risk factors prior to determining the overall risk level and the type of mitigation techniques which should be applied.

It is important to note however that Section 17 (3) (c) of the 2021 MLPA Amendment Act prohibits the implementation of simplified due diligence measures whenever there is a suspicion of ML, TF or PF.

7.0 The Risk Assessment Process

7.1 What is Risk?

Risk can be defined as the combination of the probability of an event and its consequences. In simple terms risks can be seen as a combination of the chance that something may happen and the degree of damage or loss that may result if it does occur.

7.2 What is Risk Management?

Risk management is the process of recognising risk and developing methods to both minimise and manage the risk. This requires the development of a method to identify, prioritise, treat (deal with), control and monitor risk exposures. In risk management, the identified risks must be assessed against the likelihood (chance) of them occurring and the severity or amount of loss or damage (impact) which may result if they do happen.

7.3 Which Risks must be Managed?

It is unrealistic for a reporting entity to operate in an environment free of ML/TF/PF risk. Therefore, reporting entities should conduct risk assessments to identify and assess the ML/TF/PF risk it faces, and determine the best ways to reduce and manage these risks. In doing this, it is necessary to balance the costs to the business and customers against the risk of the being used for ML/TF/PF.

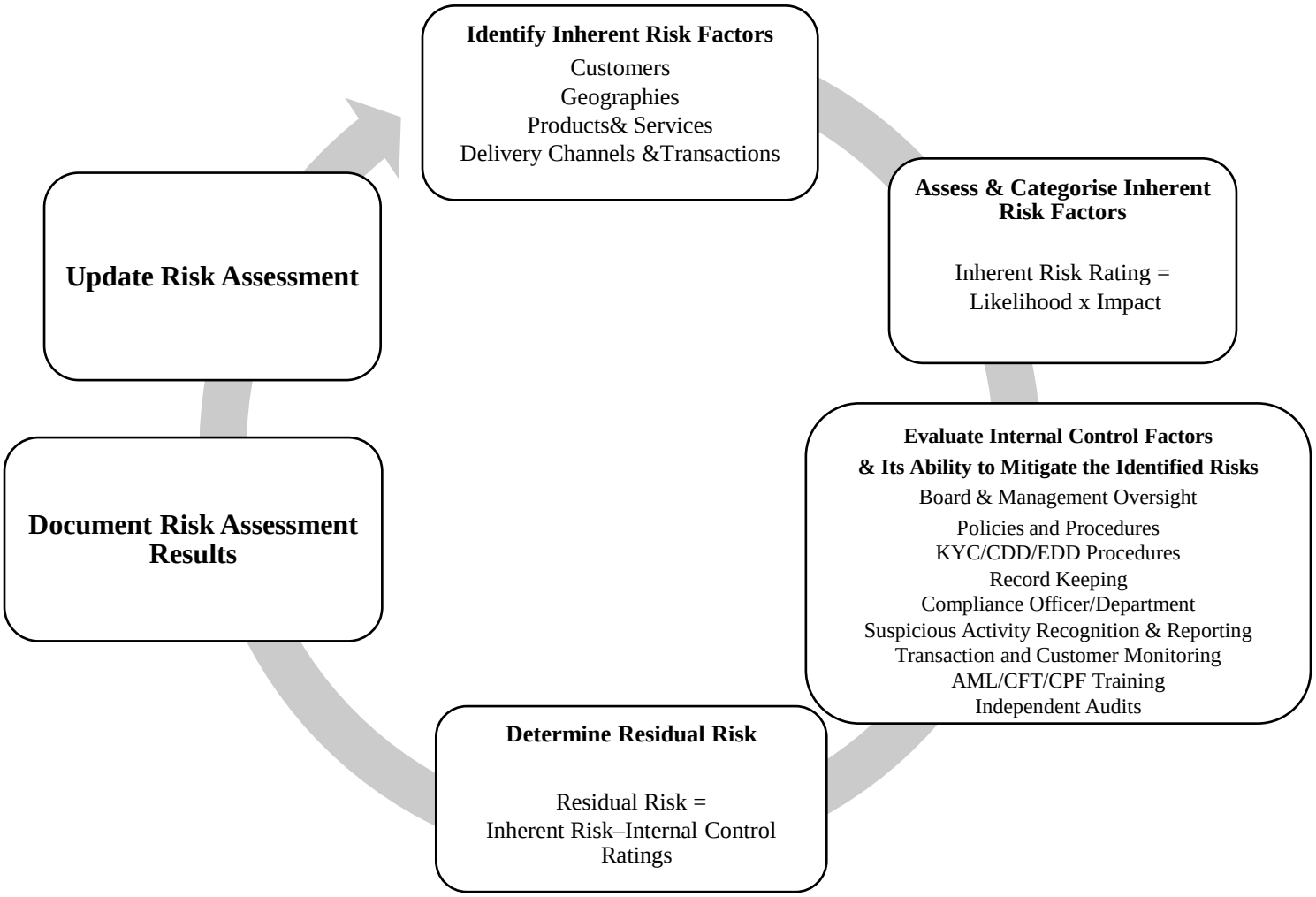
The risk assessment must be tailored to the nature, size, and complexity of the operations of the reporting entity. This means that the methodology applied by the reporting entity should account for these factors.

As part of the risk assessment process, a reporting entity must consider all relevant inherent ML/TF/PF risks factors i.e., the exposure to ML, TF and PF risk assessed before any mitigating controls have been applied. Inherent risk may increase the reporting entities' vulnerability to being abused ML, TF and PF.

The basic steps in conducting a ML/TF/ PF risk assessment consist of:

1. Identifying the inherent ML/TF/PF risks in relation to:
    - Customers (including beneficial owners)
    - Geographic Locations
    - Products and services that the reporting entity offers
    - Delivery channel of the products and services
2. Assessing the identified ML/TF/PF Risks
3. Evaluating the effectiveness of the controls designed to mitigate the identified ML/TF/PF risks
4. Determination of Residual Risk
5. Documentation of the Risk Assessment results
6. Monitoring/ Reviewing risks and updating the Risk Assessment on an on-going basis

Figure 1. The ML/TF/PF Risk Assessment Cycle



Subsequent to determining the residual risk ratings the reporting entity should assess whether it is in line with its risk appetite/tolerance. If the residual risk exceeds your

acceptable tolerance appropriate mitigation measures must be implemented in order to lower the residual risk to an acceptable level.

8.0 Identifying the ML/TF/PF Risks

The first step that reporting entities should undertake in conducting its risk assessment is to assess the ML/TF/PF risks to which the business is or may be exposed to during the conduct of its operations, before the application or implementation of any internal control measures. It is important to note that as all businesses are different in nature, size and complexity, the inherent risks will vary.

The identification process should be comprehensive but dynamic, as it should enable new or previously undetected risks to be identified and considered at any stage in the process.

In conducting the risk assessment, the reporting entity should consider the following risk factors:

- *Customer Risks* – the type of customers the reporting entity conducts business with
- *Product/Service Risks* – the type of products and/or services provided to customers
- *Geographic Risks* – the geographical location of customers and locations of the reporting entity's operations
- *Transaction and Delivery Channels Risks* – the way products and/or services are delivered to and transactions are conducted with customers
- *Other Factors* – any other risks factors as identified by the reporting entity

Each of the above factors are described in further detail below. The list is not exhaustive and as such the reporting entity may consider other pertinent risk factors applicable to the nature, size and complexity of its business.

8.1 Customer Risks

The reporting entity should understand the nature and the level of risks that their customers may bring into their business, as certain categories of customers may pose a higher ML/TF/PF risk than others. In establishing the customer risks, the following criteria may be considered:

- The customer type e.g., whether customers are individuals, legal persons or arrangements, high-net worth individuals or, politically exposed persons (PEPs)
- The ownership structure of customers who are legal persons e.g., whether the business/company has a complex ownership structure which may obscure the identity of the beneficial owner(s)
- Nature of their business activity – whether the customer's business is by nature a high-risk business (e.g., cash-intensive businesses)

8.2 Product/Service Risks

Reporting entities should assess the potential risks arising from the products and services that they offer to their customers. Certain products and services, by their nature, may

present high vulnerability to ML/TF/PF and thus may be exploited for these purposes. In assessing the risks of the products/services provided, it is recommended that the following be considered:

- whether the product/service allows for anonymity
- whether the product/service allows the identity of the beneficial owner to be obscured
- whether the product/service disguises or conceals the source of wealth or funds of the customer
- whether the product/service commonly involves the receipt or payment in cash
- whether the product/service has a high transaction or investment value
- whether the product/service has been identified domestically or internationally as presenting a higher ML/TF/PF risk

8.3 Geographic Risks

Geographical risk may arise with respect to the location or nationality of a customer or the origin and the destination of transactions conducted by the customer as different geographic locations pose different levels of AML/CFT/CPF risks, based on the prevailing factors in that particular jurisdiction.

While there is no general way to determine whether a particular country or geographical area can be classified as being more vulnerable to ML/TF/PF risk, reporting entities may consider whether the country or jurisdiction:

- has been identified as being subjected to economic sanctions or embargoes
- is known to be providing funding for or otherwise supporting terrorist activities or the proliferation of weapons of mass destruction
- lacks appropriate and effective systems to combat ML/TF/PF
- has a high level of corruption or other criminal and illicit financial activities.

The reporting entity should also consider the jurisdictions they are exposed to through their own activities or activities of their customers.

To identify such jurisdictions, country reports issued by international organisations may be considered, including but not limited to:

- The Financial Action Task Force (FATF) list of high-risk and non-cooperative jurisdictions
- FATF country mutual evaluation reports
- Transparency International Corruption Perception Index
- Organisation for Economic Cooperation and Development's ("OECD") country risk classification
- U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") sanctions list including the Specially Designated Nationals and Blocked Persons List ("SDN")

8.4 Transaction and Delivery Channel Risks

The way customers are on-boarded, products/services are provided to customers (delivery channels) and transactions are conducted, impacts the reporting entity's vulnerability to ML/TF/PF. Customers on-boarded by non-face-to-face means or through intermediaries present a higher threat to ML/TF/PF by nature due to the challenges that may occur in the verification of the customer's identity.

In assessing the risks of the products/services provided, it is recommended that the following be considered:

- Are products/services provided to customers face-to-face? i.e., customers are physically met or known personally to the business.
- Are products/services provided to customers on a non-face-to-face basis? i.e., customers are not personally met but have direct contact with the business through telephone, electronic mail, or other forms of communication.
- Are intermediaries used for the provision of products and services? i.e., there is no direct relationship with the end-customer and all transactions and communication is done through an intermediary.

In addition, reporting entities should be aware of the risks associated with the manner in which transactions with the customers are conducted. Payments conducted in cash pose a higher ML/TF/PF risk than transactions conducted through the financial system e.g., bank transfers, cheques or VISA cards.

8.5 Any Other Factors

Reporting entities may also assess other factors, which does not fall in the categories outlined above but apply to the nature of their business. Moreover, there may be features about a business that can make it more attractive to individuals who want to carry out ML/TF/PF activities. These factors must also be considered.

9.0 Assessing and Categorising the Inherent ML/TF/PF Risks

Upon identification of the relevant risks, the reporting entity should determine the level of those risks within its business. The objective of this stage is to gain a comprehensive understanding of each risk factor that has been identified and consideration of the likelihood and impact of each risk factor based on the reporting entities' experience such as historical/present data and publicly available information such as NRA.

Having identified all ML/TF/PF risk factors, the reporting entity must assess/measure each risk factor in terms of the likelihood (chance) they will occur and the severity or amount of loss or damage (impact) which may result if they do occur. The inherent risk is determined by multiplying the likelihood of occurrence of the risk factor by the impact (seriousness of the damage) it may cause. Each risk factor can be rated in terms of:

- the chance of the risk happening – 'likelihood'
- the amount of loss or damage if the risk happened – 'impact' (consequence)

To help assess each risk factor, the reporting entity may apply risk rating scales for the likelihood of occurrence depicted in Table 1 below and impact of the occurrence depicted in Table 2 below, from which a risk score can be calculated.

The ratings applied to each factor based on likelihood and impact is likely to vary from product to product and customer to customer (or category of customer) and from one reporting entity to another. Accordingly, the risk ratings should be consistent with the size, type, and complexity of the business.

9.1 Likelihood Scale

A likelihood scale refers to the potential of an ML/TF/PF risk occurring in the reporting entity for the particular risk being assessed. Three (3) levels of risk are shown in Table 1, but the reporting entity can have as many as they believe are necessary.

Table 1: Likelihood of a Risk Factor Happening

Rating	Likelihood of ML/TF/PF Risk
Likely	High probability that the risk is present
Possible	Reasonable probability that the risk is present
Unlikely	Unlikely that the risk is present

In order to establish the reporting entity's exposure to ML/TF/PF and the efficient management of that risk, the reporting entity needs to identify every segment of its operations where it may be susceptible to ML/TF/PF. The size and complexity of a reporting entity plays an important role in how attractive or susceptible it is for ML/TF/PF. For example, a large business is less likely to know a customer personally who thereby can be more anonymous than a customer of a small organisation. An organisation that provides international services might be more attractive to a money launderer than an organisation that only provides domestic services.

9.2 Impact Scale

An impact scale refers to the seriousness of the damage (or otherwise) which could occur should the risk occur. Impact of an ML/TF/PF risk could, depending on the reporting entity's circumstances, be rated or looked at from the following points of view:

- how it may affect the reporting entity (if through not dealing with risks properly the entity suffers a financial loss from either a crime or through fines from the regulator)
- the risk that a particular transaction may result in the loss of life or property through a terrorist act
- the risk that a particular transaction may result in funds being used for criminal conduct including any of the following: corruption, bribery, smuggling of goods/workers/immigrants, banking offences, narcotics offences, psychotropic substance offences, illegal arms trading, kidnapping, terrorism, theft, embezzlement, or fraud

- the risk that a particular transaction may cause suffering due to the financing of illegal drugs
- reputational risk – how it may affect the reporting if it is found to have (unknowingly) aided an illegal act, such as sanctions being imposed and/or being shunned by the community of customers
- how it may affect the wider community of customers if it is found to have aided an illegal act; the community may get a bad reputation as well as the reporting entity

The above list does not cover every possible scenario and it is not prescriptive.

Table 2: The Impact/Severity of the Event Occurring

Rating	ML/TF/PF Impact
Minor	The risk has minor or no consequences. Can be used directly or indirectly to fund or support criminal activities with minor impact.
Moderate	The risk has moderate consequences. Can be used directly or indirectly to fund or support criminal activities with moderate impact.
Significant	The risk has severe consequences. Can be used directly or indirectly to fund or support criminal activities with a significant impact.

Three (3) levels of risk are shown in Table 2, but the entity can have as many as they believe are necessary.

An assessment of ML, TF and PF risks proceeds from the assumption that the different products and services offered, or the different transactions executed by the reporting entity, are not equally vulnerable to misuse by criminals. The purpose of a risk assessment is to apply control measures proportionate to the identified risk. This allows reporting entities to focus on the customers, countries, products, services, transactions and delivery channels that constitute the greatest potential risk.

9.3 Inherent Risk as a Function of Likelihood and Impact

A risk matrix can then be used to combine likelihood and impact to obtain a risk score. The risk score may be used to aid decision making and help in deciding what action to take in view of the overall risk.

Table 3: Inherent Risk Matrix

Inherent Risk Assessment		Impact		
		Minor	**Moderate**	**Significant**
Likelihood	**Unlikely**	Low	Low	Medium
	Possible	Low	Medium	High
	Likely	Medium	High	High

Reporting entities should ensure that they understand how their risk rating system works, whether it is a manual or automated system, and how it combines, or weighs, risk factors

to achieve overall risk scores. Reporting entities should also be able to satisfy the FIA that it understands the system used for assessing ML/TF/PF risks and that the system reflects its understanding of these risks.

EXAMPLE ONLY

Table 4: Examples of Risk Factors and Risk Descriptions

Risk Factor	Risk Description
Customer is a small business	A customer who is a small business are usually domestic with simple ownership structures. Most of these businesses deal with cash and multiple persons can be acting on their behalf. The **likelihood** that funds deposited are from illegitimate source is **possible.** If a reporting entity has a large number of customers that are small businesses, then the **impact** can be **'significant'**. Thus, the inherent risk will be '**high'**.
Customer is an international cooperation	Customers that are international corporations have complex ownership structures with often foreign beneficial ownership. If a reporting entity has only a few of those customers, which are mostly located offshore then the **likelihood** of ML, TF or PF will be **'likely'**, however, because of the limited number of customers the **impact** will be **'moderate'**. Thus, the inherent risk will be **'medium'**.
Life Insurance Product	Life insurance products are simple and premiums tend to be very low. They are only sold to resident persons only. If a reporting entity receives premium payments mostly by salary deductions with little cash involved. The **likelihood** that the life insurance product is used for ML/TF/PF is **'unlikely'** and the **impact** will be **'minor'**. Thus, the inherent risk will be **'low'**.

10.0 Evaluating AML/CFT/CPF Internal Controls

In this step, internal controls must be evaluated to determine how effectively they offset the identified risks. Controls include the programmes, policies or activities put in place by the reporting entity to protect against the materialisation of a ML /TF/PF risk, or to ensure that potential risks are promptly identified. Controls are also used to achieve compliance with the MLPA.

The controls in place are evaluated for their effectiveness in mitigating the inherent risks and to determine the residual risk ratings. AML/CFT/CPF controls should be assessed across the following control categories (as applicable):

- Corporate Governance; Board & Management Oversight
- Policies and Procedures
- KYC/CDD/EDD Procedures
- Record Keeping
- Compliance Officer/Department

- Suspicious Activity Recognition and Reporting
- Transaction and Customer Monitoring
- AML/CFT/CPF Training
- Independent Audits

Further details of the necessary internal controls can be found in the FIA's *'Guidance to Financial Institutions and Other Business Activities on the AML/CFT/CPF Compliance Programme'* which is available on the FIA's website.

10.1 Internal Control Factors

Each control should be assessed for its overall design and operating effectiveness. Internal Controls may be assessed as satisfactory, needs improvement or unsatisfactory and the criteria for the assessments must be documented. If controls are highlighted as either not designed or operating effectively or do not exist, it would be appropriate to raise an action to remedy this if an action is not already underway. Table 5 below provides an example of an internal control assessment which can be used:

Table 5: Internal Control Assessment Factor Scale

Satisfactory	Control(s) evaluated, designed, and operating adequately, appropriately, and effectively
Needs Improvement	A few specific control design and operating weaknesses, some of which are significant have been identified.
Unsatisfactory	Numerous specific deficiencies in control design and performance, including the absence of alignment with the MLPA. Controls evaluated are inadequate, inappropriate, or ineffective to manage the risks ML, TF and PF.

11.0 Determination of Residual Risk

Residual risk is the risk remaining after taking into consideration risk mitigation measures and controls. It is determined by 'subtracting' the level of control from inherent risk. The residual risk rating is used to indicate whether the ML/TF/PF risks within the reporting entity are being adequately managed/mitigated. It is important to note that no matter how robust the risk mitigation and risk management program, the reporting entity will always have some exposure to residual ML/TF/PF risks which must be managed.

Reporting entities may apply a three (3) level rating scale of high, medium and low to evaluate the Residual Risk. The following definitions could be considered to describe the level of residual risk applied to a three (3) level rating scale:

- **Low Residual Risk**: The inherent risk of the reporting entity's customers, products/services, channels, geographies and other qualitative factors, is low-to medium and the mitigating controls are sufficient to manage this inherent risk.
- **Medium Residual Risk**: The inherent risk of the reporting entity's customers, products/services, channels, geographies and other qualitative factors, is low-to medium and the mitigating controls are not adequate to manage this level of risk, or the overall inherent risk of the reporting entity, based on the customers, products/services, channels, geographies and other qualitative factors, is high and the mitigating controls are adequate to manage this inherent risk.
- **High Residual Risk**: The inherent risk of the reporting entity's customers, products/services, channels, geographies and other qualitative factors, is medium to-high and the mitigating controls are not sufficient to manage this inherent risk.

After determining residual risk, reporting entities should verify whether it is within the boundaries of its risk appetite, that is, determine the level which your institution is prepared to accept the remaining residual risk. If this residual risk is not within the boundaries of the reporting entity's risk appetite, additional control measures should be implemented to further reduce or avoid the risk. It should be noted that the goal is not to reduce the risk to zero, as in most cases this would be impossible.

Table 6 below provides a methodology to determine residual risk taking into consideration the inherent risk factors and the assessment of the internal controls.

Table 6: Residual Risk Matrix

Residual Risk Assessment		**Inherent Risk**		
		Low	**Medium**	**High**
Control Effectiveness	Satisfactory	Low	Low	Medium
	Needs Improvement	Low	Medium	High
	Unsatisfactory	Medium	High	High

The residual risk rating table above illustrates that:

- A strong control environment can lower the residual ML/TF/PF risk in comparison to the inherent risk
- If the reporting entity receives a High inherent ML/TF/PF risk rating, it can never achieve a Low residual ML/TF/PF risk rating
- In order to improve its residual ML/TF/PF risk, either the inherent ML/TF/PF risk must be reduced or the AML/CTF/CPF controls must be strengthened

12.0 Documentation of the ML/TF/PF Risk Assessment Results

Section 16B (2) (a), (c) and (d) of the MLPA Amendment Act states that the reporting entity must document the outcome of the risk assessment, keep it up to date and must develop appropriate mechanisms to provide risk assessment information to the FIA.

It is recommended that the results of the risk assessment and any measures undertaken by the reporting entity to mitigate the identified risks should be consolidated within a comprehensive report and communicated to the reporting entity's Board of Directors/Owners and Senior Managers. This will assist them in making informed decisions on the strategic direction of the company. In addition, the report should clearly indicate proposed action points to be adopted by the reporting entity.

Once documented, the reporting entity should ensure that:

- the risk assessment is approved by Board of Directors/Owners and Senior Managers (if applicable)
- policies and procedures established to mitigate the identified risks should be documented in the reporting entity's AML/CFT/CPF Compliance Manual and effectively implemented by the reporting entity and its staff
- ensure that senior managers, and employees are adequately informed and trained on the relevant policies and procedures implemented

13.0 Updating of the ML/TF/PF Risk Assessment

The level of ML/TF/PF risk to which a reporting entity is exposed will continuously change (either increase or decrease) depending on its nature and purpose of business, its customers' profile, the products/services it offers, and the delivery channel of these products/services to its customers.

Reporting entities should describe the process for updating the risk assessment ideally in its AML/CFT/CPF Compliance Manual. Systems and controls should be put in place to keep the assessments of the ML/TF/PF risks under review and to ensure it remains up to date and relevant. In updating the risk assessment, the factors which should be considered include:

- the type or categories of customers which the reporting entity provides products/services
- the type of products or services being offered to customers
- the manner in which products and services are provided (i.e., delivery channels) to customers
- the transaction methods used by customers
- new or emerging risks identified in the NRA that may significantly change the risk profile of reporting entity

Appendix 1: Description of Risk Factors

The tables below describe risk factors that reporting entities may consider when conducting ML/TF/PF risk assessments. It is to be noted that the list is not exhaustive and that not all risk factors outlined will be relevant or applicable to the reporting entity.

1. Nature, Size and Complexity of the Reporting Entity

Risk Factor	Risk Consideration
Size of the reporting entity	The larger your entity, the higher the risk that suspicious activities and transactions may be undetected. Large organisations may have difficulty tailoring their AML/CFT/CPF measures to meet AML/CFT/CPF requirements. Increased size (due to large number of staff) may also result in reduced adequacy and effectiveness of AML/CFT/CPF measures.
Complexity of the reporting entity	Greater complexity decreases the transparency of transactions and activities, increases ML/TF/PF vulnerability and may reduce the effectiveness of AML/CFT/CPF measures.
Nature of reporting entity's business	Certain types of businesses are more vulnerable to being misused for ML/TF/PF purposes. Further information on risks specific to the nature of a reporting entity's activities may be found in the NRA.

2. Customers Risk Factors

Risk Factor	Risk Consideration
Ownership structure of customer	Legal persons with complex and non-transparent structures may hide and disguise beneficial ownership and mask ML/TF/PF activities. In addition, customers may establish legal entities in multijurisdictional structures to hide the true ownership and control of assets held overseas. Organisational structure charts may assist in identifying beneficial ownership and effective control.
Jurisdiction in which customer resides	See the geographic risk factors section
Customers who are PEPs	PEPs may mean greater vulnerability to ML/TF/PF. By nature of positions they hold, PEPs may be considered high-risk, as they can use their positions to influence individuals and institutions and facilitate the movement of funds. Their privileged position (access to state funds and decision-making) heightens ML/TF/PF risks. In addition. PEPs may also seek to obscure their financial position using their relatives or close associates.

Nature of customer's business or customer occupation	Some businesses/occupations pose a greater vulnerability to ML/TF/PF. E.g., cash intensive businesses and gatekeeper occupations.

3. Products and Services Risk Factors

Risk Factor	**Risk Consideration**
Products/Services geared towards foreign/offshore customers	Offshore customers may expose reporting entities to higher ML/TF/PF risk, especially in connection with countries with high levels of corruption, bribery, organised crime and also with weak AML/CFT/CPF regimes
Features of product or service	Legitimate products and services can be used to mask the origins of illegal funds and to hide the identity of the owner or beneficiary of the products or services. Consideration should therefore be given to the market in which the reporting entity operates and to whom the products or services are directed. The type of business or individuals to whom the products and services are directed determines the impact of these risk factors. Examples include products and services offered through intermediaries or agents. Certain products and services lend themselves more easily to abuse by customers and third parties such as online transactions/funds transfers.
Products/services provided support the pooling of funds and investments.	This can disguise the beneficial ownership of funds. It can enable criminals to place money within the financial system with fewer questions being asked because of the perceived respectability and legitimacy of the source of funds. It can also act as the link between different ML/TF/PF techniques, such as purchasing real estate.
New technologies such as quick anonymous payments	Reporting entities must consider the products or services that are based on new technologies and their impact on them. Examples of payment methods used to transmit funds more quickly or anonymously include e-wallets, pre-paid cards, internet payment services, digital currency, or mobile payments.

4. Geographic Location Risk Factors

Risk Factor	Risk Consideration
Customers from countries that have a weak or ineffective AML/CFT/CPF measures	Reporting entities should consider variables such as customers from countries with lesser AML/CFT/CPF provisions, weak regulations and law enforcements. Reporting entities should consult the various Mutual Evaluation Reports conducted by the FATF in respect of the countries from which their customers reside and other relevant AML/CFT/CPF publications for identification of countries/jurisdictions with AML/CFT/CPF deficiencies.
Customers from countries that have generally high ML/TF/PF risks	Factors which should be considered include whether the countries/jurisdictions: • have a cash intensive economy • is a source of or renowned for illicit activities (organised crimes or drug-related crimes) • has an unstable or weak government In addition, consideration should also be given to countries identified by credible sources as providing funding for or otherwise supporting terrorist activities.
Customers from countries that are subjected to sanctions	Sanctions may apply to dealings with countries, terrorist organizations or designated persons from a target country and can impact a reporting entity by: • Prohibiting trade and other economic activity with a foreign market • Restricting financial transactions • Leading to seizure of property in both the domestic and other jurisdictions. The extent to which a reporting entity is impacted by international sanctions must be considered. The following listings may be used to determine countries on which sanctions have been imposed • Security Council Resolutions: https://www.un.org/securitycouncil/content/resolutions • Consolidated list of persons, groups, and entities subject to EU financial sanctions: https://data.europa.eu/euodp/en/data/dataset/consolidated-list-of-persons-groups-and-entities-subject-to-eu-financial-sanctions • High Risk and Non-Cooperative Jurisdictions: http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/?hf=10&b=0&s=desc(fatf_releasedate)

5. Delivery Channel Risk Factors

Risk Factor	Risk Consideration
Methods of delivery used for products and services that provide for anonymity	Anonymity is highly sought after by criminal elements to facilitate ML/TF/PF. Accordingly, a major part of your AML/CFT/CPF measures should be focused on removing anonymity and increasing transparency.
Products and services obtained through intermediaries or third parties	This may result in the customer's identity, beneficial owner or effective controller not being transparent to the reporting entity.
Non face to face contact with customer	Less face-to-face interaction with a customer increases vulnerability to ML/TF/PF activity.
Payments to/from third parties or non-customers	This can disguise the beneficial ownership or effective control of funds. The presence of multiple intermediaries and agents can hide and disguise beneficial ownership.
Acceptance of high value payments through cash transactions	Cash payments may obscure the origins of the source of the funds. Cash-intensive businesses are attractive to criminals as it allows for illicit funds to be mingled with legitimate sources of funds
Acceptance of partial payments and structured payments in cash	This may result in criminals taking advantage of partial/structured payments below reporting thresholds to avoid detection or raising a red flag.

End of Document