THE FINANCIAL INTELLIGENCE CENTRE

# GUIDELINES FOR CONDUCTING INSTITUTIONAL MONEY LAUNDERING/TEORRORIST FINANCING/PROLIFERATION FINANCING (ML/TF/PF) RISK ASSESSMENT

2021

## 1.0 INTRODUCTION

In keeping with international obligations and ensuring that Zambia's Financial Service Providers (FSPs) and other non-financial businesses and professions are not abused by persons involved in money laundering (ML) or the financing of terrorism ( TF), the Financial Intelligence Centre ('the FIC ') was established to receive suspicious transaction reports (STRs) from reporting entities, analyze and disseminate intelligence reports to law enforcement agencies (LEAs), pursuant to the Financial Intelligence Centre Act No. 46 of 2010 ( 'the Act')(as amended).

One of the responsibilities of reporting entities as provided for under section 19 (1) of the FICAct No. 46 of 2010 (as amended) is to undertake the Money Laundering (ML), Terrorist Financing (TF) and Proliferation Financing (PF) risk assessment (for customers, country or geographic locations, products/services, transactions or delivery channels) . The guidelines have been issued in accordance with section 56 and pursuant to section 19 of the FIC Act No. 46 of 2010 (as amended).

## 2.0 PURPOSE OF THE MONEY LAUNDERING/ TERRORIST FINANCING/ PROLIFERATION FINANCING RISK ASSESSMENT GUIDELINES

The purpose of these Guidelines is to assist reporting entities in conducting their Money Laundering/ Terrorist Financing /Proliferation Financing (ML/TF/PF) risk assessment. The Guidelines outline minimum requirements in respect of the institutional ML/TF/PF risk assessment. The Institutional ML/TF/PF Risk Assessment guidelines are structured to help reporting entities identify their risks by products, services and delivery channels; customers and business relationships; geography and other relevant factors. In addition, the guidelines will assist reporting entities implement effective measures and monitor ML/TF/PF risks that they may encounter as part of their activities and business relationships.

## 3.0 SCOPE

These Guidelines set the minimum standards that institutions should adopt to develop an effective ML/TF/PF risk assessment framework. The guidelines do not replace nor supersede the legislation or regulations that reporting entities must comply with as part of their regulatory obligations.

## 4.0 DEFINITION OF KEY TERMS

For the purpose of these Guidelines, the following definitions shall apply:

**Financial Action Task Force** (FATF): Is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter terrorist and proliferation financing (CTFP) standard.

**Money Laundering**: Under The Prohibition and Prevention of Money Laundering Act No 14 of 2001, as amended by Act No.44 of 2010, a money laundering offence involves various acts committed with the intention to conceal or convert property or the proceeds of property (e.g. money) knowing or believing that these were derived from the commission of a designated offence. In this context, a designated offence means a serious offence as defined in the Forfeiture of Proceeds of Crime Act, 2010. It includes among others those relating to illegal drug trafficking, corruption, bribery, fraud, forgery, murder, robbery, counterfeit money, stock manipulation. A money laundering offence may also extend to property or proceeds derived from illegal activities that took place outside Zambia.

**Prominent Influential Persons (PIPs)**: Are individuals who are or have, been entrusted with a prominent public function by a State or an international or local body or organisation but are not of middle or junior ranking.

**Proliferation Financing**: means an act by any person who by any means, directly or indirectly, willfully or negligently provides funds or financial services to be used or knowing that they are to be used in whole or in part for proliferation, the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling, supply, sale or use of nuclear, ballistic, chemical, radiological or biological weapons or any other weapon capable of causing mass destruction and their means of delivery and related materials including both technologies and dual-use goods used for non-legitimate purposes, including technology, goods, software, services or expertise.

**Reporting Entity**: An institution regulated by a Supervisory Authority and required to make a suspicious transaction report to the Centre on suspected Money Laundering, Terrorism and Proliferation Financing and other serious offences related to money laundering, terrorism and proliferation financing under the Act.

**Risk Based Approach:** Identification of the money laundering, terrorist and proliferation financing risks of customers and transactions which allow us to determine and implement proportionate measures and controls to mitigate these risks.

**Suspicious Transaction Report:** a report submitted on suspected money laundering, terrorism and proliferation financing or other serious offence, or attempted money laundering, terrorism and proliferation financing or other serious offence, whether in form of a data message or otherwise.

**Terrorist Financing**: Terrorist financing offences extend to any person who wilfully provides or collects funds by any means, directly or indirectly, with the unlawful intention that they should be used or in the knowledge that they are to be used in full or in part to carry out a terrorist act by a terrorist organization or an individual terrorist. Under the Anti-Terrorism Act No. 21 of 2007 (as amended), it is an offence to knowingly collect or provide property, such as funds, either directly or indirectly, to carry out terrorism or terrorist financing activities.

**Inherent Risk:** refers to risk that exists before the application of controls or mitigation measures.

**Impact:** this refers to the extent of the damage that would occur if the ML/TF risk materializes (i.e. threats and vulnerabilities).

**Mitigation measures:** Controls put in place to limit the potential money laundering and terrorist and proliferation financing risks identified while conducting a risk assessment.

**Residual risk:** the level of risk that remains after the implementation of mitigation measures and controls.

**Risk:** can be defined as the likelihood of an event and its consequences. In the context of money laundering/terrorist and proliferation financing (ML/TF/PF), risk means:

- ❖ **At the national level:** threats and vulnerabilities presented by ML/TF/PF that put at risk the integrity of Zambia's financial system and the safety and security of Zambians**.**
- ❖ **At the reporting entity level:** threats and vulnerabilities that put the reporting entity at risk of being used to facilitate ML/TF/PF.

**Risk factors:** means variables that, either on their own or in combination, may increase or decrease the ML/TF/PF risk posed by an individual business relationship or occasional transaction.

**Risk-based approach:** means an approach whereby competent authorities and firms identify, assess and understand the ML/TF/PF risks to which firms are exposed and take AML/CFPT measures that are proportionate to those risks.

**Threats:** this could be a person (or group), object that could cause harm. In the ML/TF context, a threat could be criminals, facilitators, their funds or even terrorist groups.

**Vulnerabilities:** elements of a business that could be exploited by the identified threat. In the ML/TF/PF context, vulnerabilities could be weak controls within a reporting entity, offering high risk products or services, etc.

## 5.0 HOW TO ASSESS MONEY LAUNDERING/TERRORIST FINANCING/ PROLIFERATION FINANCING RISKS

As part of assessing ML/TF/PF risk, a reporting entity needs to identify the areas of its business that are vulnerable to being used by criminals for conducting ML/TF/PF activities.

This means that a reporting entity has to assess the risks associated with all its business services and activities. Specifically, it must address the following four areas:

i. your customers or Clients (Customer/Clients risks)
ii. your products and services (product/service risks)
iii. your business practices/delivery methods (business practices/channels risks)

iv. the countries a reporting entity does business in or with (jurisdictions/geographical risks).

The following are some examples that may influence the level of risk that you may find for each category.

A. **Customers**

i. Prominent Influential Persons
ii. a non-resident customer;
iii. a private banking customer;
iv. a legal person or legal arrangement that is a personal asset holding vehicle;
v. a company that has a nominee shareholder or shares in bearer form; or
vi. a customer that performs a transaction on behalf of another person, whether the identity of such other person is disclosed or not.
vii. the type of customer – for example, an individual, sole trader or company etc.
viii. new customers
ix. customers who want to carry out large transactions
x. a customer or group of customers making lots of payments to the same recipient
xi. customers who have a business which involves large amounts of cash
xii. a customer whose identification is difficult to check
xiii. customers who use large amounts of bank notes and/or small denominations.

B. **Products and services**

i. remittance services
ii. gambling/wagering account
iii. superannuation fund account
iv. digital currency exchange
v. private banking products.
vi. Tax services

C. **Business practices/delivery channels**

i. Non-face to face
ii. online/internet
iii. phone
iv. email

v. third-party agent or broker.

**D. Countries/jurisdictions**

i. any country or particular region of a country in which you may do business
ii. any country subject to trade sanctions or other United Nations sanctions
iii. any country known to be a tax haven, source of narcotics or other significant criminal activity.
iv. Any country identified by the Financial Action Task Force as having strategic AML/CTPF deficiencies.

If a reporting entity identifies situations that represent a high risk for ML/TF/PF activities, it should control these risks by implementing mitigation measures.

### 5.1 CUSTOMER/CLIENT RISK ASSESSMENT

This should be assessed for the purposes of identifying the inherent money laundering, terrorism and proliferation financing risk of an institution's client base and business relationship. An institution shall determine, based on its own criteria, what risks a particular customer poses. Certain customers and entities may pose specific risks depending on the nature of the business, the occupation of the customer and the nature of anticipated transaction activity.

Some factors to consider are:

a. Customers conducting their business relationship or transactions in unusual circumstances, such as:
    i. Significant and unexplained geographic distance between the institution and the location of the customer;
    ii. Frequent and unexplained movement of accounts to different institutions; and;
    iii. Frequent and unexplained movement of funds between institutions in various geographic locations.
b. Customers whose structure or nature of the entity or relationship makes it difficult to identify the true owner or controlling interests.
c. Prominent Influential Persons (PIPs). Individuals who are or have been entrusted with prominent public functions (both foreign and local), for example, senior politicians, senior government officials, judicial or military officials, senior executives of state owned corporations, important political party officials. Business relationships with family members or close associates of PIPs may involve reputational risks similar to those with PIPs.
d. Accounts held by non-residents and foreign individuals.

e. Business relationships entered into with non-residents and foreign individual
f. Foreign corporations and domestic business entities, particularly offshore corporations such as domestic shell companies, private investment companies and international business corporations located in high-risk geographic locations.
g. Cash-intensive businesses, including, for example, supermarkets, convenience stores, restaurants, retail stores, liquor stores, wholesale distributors, car dealers among others.
h. Foreign and domestic non-governmental organizations and charities.

Reporting Entities should develop a worksheet to capture the customer risk assessment based on the inherent characteristics of its clients. The worksheet should as a minimum have columns on; the Customer Type, Risk Rating (Scores), Mitigation/ Controls, Weights used and the Residual Risk.

Below is the table to illustrate.

Table 1: Customer Risk Assessment Worksheet

| **Customer Type** | **Weights Used** | **Risk Rating (Scores)** | **Mitigation /Controls** | **Residual Risk** |
|---|---|---|---|---|
| Prominent Influential Persons (PIP) | **Likelihood**=Very Likely(3)<br>**Impact**= Moderate(2) | **High (6)** | • Enhanced monitoring and Customer Due Diligence<br>• Senior Management Approval | Medium |

## 5.2 PRODUCTS AND SERVICES RISK ASSESSMENT

Institutions should consider the potential money laundering and terrorism and proliferation financing risks associated with each of its specific product or service. An institution will seek to identify its portfolio of products/account types and assign an inherent score to each, based on its general inherent characteristics and the degree of money laundering and terrorism and proliferation financing risk present. Some factors to consider are:

**a) the level of transparency or opaqueness, the product, service or transaction affords;**

The reporting entity should determine to what extent do products or services allow the customer or beneficial owner or beneficiary structures to remain anonymous, or facilitate hiding their identity? Examples of such products and services include bearer shares, fiduciary deposits, offshore investments and certain trusts, and legal entities such as foundations that can be structured in such a way as to take advantage of anonymity and allow dealings with shell companies or companies with nominee shareholders. Further, the reporting entity should determine to what extent is it possible for a third party that is not part of the business relationship to give instructions, for example in the case of certain correspondent banking relationships?

**b) the complexity of the product, service or transaction;**

The reporting entity should determine to what extent is the transaction complex and does it involve multiple parties or multiple jurisdictions, for example in the case of certain trade finance transactions? Are transactions straightforward, are regular payments made into a pension fund?

To what extent do products or services allow payments from third parties or accept overpayments where this is would not normally be expected? Where third party payments are expected, does the firm know the third party's identity, for example is it a state benefit authority or a guarantor? Or are products and services funded exclusively by fund transfers from the customer's own account at another financial institution that is subject to AML/CFT standards and oversight that are comparable to those required under the FIC Act? Does the firm understand the risks associated with its new or innovative product or service, in particular where this involves the use of new technologies or payment methods?

**c) the value or size of the product, service or transaction.**

The reporting entity should determine to what extent are products or services cash intensive, as are many payment services but also certain current accounts? To what extent do products or services facilitate or encourage high-value transactions? Are there any caps on transaction values or levels of premium that could limit the use of the product or service for ML/TF purposes?

In undertaking this assessment, the institution is required to list all its products, identify Inherent Risks, Mitigation/Controls, Scores (Risk Level), Weights used and the Residual Risk.

## 5.3 DELIVERY CHANNELS RISKS ASSESSMENT

Institutions have various modes of transaction and distribution (delivery channels) of its products and services. Some delivery channels may be more susceptible to ML/TF/PF risk. Consequently it should be assessed whether, and to what extent, the method of delivery, such as non-face-to-face or the involvement of third parties, including intermediaries and agents, could increase the inherent money laundering risk. In undertaking this assessment, the institution is required to list all delivery channels, identify Inherent Risks, Rationale, Mitigation/ Controls, Scores, Weights used and the Residual Risk.  Some factors to consider are:

a) the extent to which the business relationship is conducted on a non-face-to-face basis;
b) any introducers or intermediaries the reporting entity might use and the nature of their relationship with the reporting entity.
c) whether the customer physically present for identification purposes. If they are not, whether the firm
    i) considered whether there is a risk that the customer may have sought to avoid face-to-face contact deliberately for reasons other than convenience or incapacity;
    ii) used a reliable form of non-face-to-face CDD; and
    iii) taken steps to prevent impersonation or identity fraud.

d) whether the customer has been introduced by a third party, for example a bank that is not part of the same group or an intermediary, and if so
    i) whether the third party is a regulated entity subject to AML obligations that are consistent with those of the FIC Act.
    ii) whether the third party applies CDD measures, keeps records to FIC Act requirements, is supervised for compliance with comparable AML/CFT obligations in line with the FIC Act.
    iii) whether the third party is based in a jurisdiction associated with higher ML/TF risk.

In undertaking this assessment, the institution is required to identify risks and explain the risk scoring allocated to each delivery channel highlighted. The assessment should also indicate: Mitigation/ Controls, Scores (Risk Level), Weights used and the Residual Risk.

## 5.4 GEOGRAPHY/COUNTRY RISK ASSESSMENT

This involves identifying geographic locations that may pose a higher risk to a reporting entity's business. An institution will seek to understand and evaluate the specific risks associated with doing business in or offering products and services and/or facilitating transactions involving certain geographic locations. The Geography/Country risk may also be analysed with respect to the location of the business division, unit or business line, and may also include its subsidiaries, affiliates and offices, both internationally and domestically.

Reporting entities should identify domestic and international geographic locations that may pose a higher risk to its AML/CFT compliance program.

Factors that may result in a country or region posing a higher risk include:

a) Countries that are subject to sanctions, embargoes or similar measures issued by credible organizations such as the United Nations and the Financial Action Task Force.
b) Countries identified by credible sources as lacking appropriate AML/CFT laws, regulations and other measures.
c) Countries identified by credible sources as providing funding or support for terrorist activities or that have designated terrorist organisations operating within them.
d) High crime areas as they may present additional ML/TF/PF risks.

A rural area where clients are known to you could present a lesser risk compared to a large city where new clients and anonymity are more likely. However, the known presence of organized crime in a rural area would obviously present a higher risk. Is the business close to a border-crossing? Proximity to a border-crossing could increase the risk due to the fact that your business may be the first point of entry into the financial system.

In undertaking this assessment, the institution is required to identify risks and explain the risk scoring allocated to each geographical area highlighted. The assessment should also indicate: Mitigation/ Controls, Scores (Risk Level), Weights used and the Residual Risk.

## 5.5 OTHER RISK FACTORS TO CONSIDER

When formulating the risk assessment, reporting entities should also assess additional risk factors that can have an impact on operational risks and contribute to an increasing or decreasing likelihood of breakdowns in key AML/CFT controls. These risk factors that may directly or indirectly affect inherent risk factors may include:

i) Significant strategy and operational changes.
ii) Structure of ownership/ business e.g. presence of subsidiaries.
iii) National Risk Assessments.

### 5.6 DETAILED ANALYSIS OF THE RISK ASSESSMENT

Once a reporting entity has identified the risk, the next step of the risk assessment process entails a more detailed analysis of the data obtained during the identification stage in order to more accurately assess ML/TF risk.

This step involves evaluating data pertaining to the reporting entity's activities (e.g. number of domestic and international transactions, types of customers, geographic locations of the reporting entity's business area and customer transactions).

This detailed analysis is ultimately important because within any type of product/service or category of customer there will be clients that pose varying levels of risk. This step in the risk assessment process gives management a better understanding of the reporting entity's risk profile in order to develop the appropriate policies, procedures, and processes to mitigate the overall risk.

#### 5.6.1 Weights and Scoring

Due to the nature of each institution's unique business activities, products and services (including transactions), client base and geographic footprint, a risk based approach is used to calculate inherent risks. Each risk factor is usually assigned a score which reflects the associated level of risk. Each risk area may then be assigned a weight which reflects the level of importance in the overall risk calculation relative to other risk areas.

The weight assigned to each of these risk categories (individually or in combination) in assessing the overall risk of potential money laundering may vary from one institution to another, depending on their respective circumstances. Consequently, an institution will have to make its own determination as to the risk weights and scores to assign to the different risk (refer to section **5.6.4**).

### 5.6.2 Risk Mitigation

The reporting entity must develop and implement policies and procedures to mitigate the ML/TF/PF risks they have identified through their institutional risk assessments. The mitigation measure should include;

- internal policies, procedures and controls to fulfil obligations under the FIC Act;
- adequate screening procedures to ensure high standards when hiring employees;
- ongoing training for officers and employees to make them aware of the laws relating to money laundering, the financing of terrorism or proliferation
- policies and procedures to prevent the misuse of technological developments including those related to electronic means of storing and transferring funds or value;
- mechanisms for preventing money laundering, financing of terrorism or proliferation, or any other serious offence;
- independent audit arrangements to review and verify compliance with and effectiveness of the measures taken in accordance with this Act;
- risk based approach to managing ML/TF/PF risks identified
- customer identification procedures;
- record keeping and retention;
- reporting procedures;
- confidentiality requirements and procedures;
- transaction monitoring systems; and
- adequate screening procedures for customers against relevant sanctions lists.
- enhanced identification, verification and ongoing due diligence procedures with respect to customers who have been identified as high risk customers.

### 5.6.3 Residual Risk

Once both the inherent risk and the effectiveness of the internal control environment have been considered, the residual risk should be determined. Residual risk is the risk that remains after controls are applied to the inherent risk. It is determined by balancing the level of inherent risk with the overall strength of the risk management activities/controls. The residual risk rating is used to indicate whether the ML/TF risks within the institution are being adequately managed.

For example, a 3 tier rating scale can be applied to evaluate the residual risk on a scale of High, Medium and Low.

### 5.6.4 Assessing and measuring risks

Once you have identified the risks your business faces, each risk needs to be assessed and measured in terms of the chance (likelihood) it will occur and the severity or amount of loss or damage (impact) which may result if it does occur.

The risk level associated with each event is a combination of the likelihood that the event will occur and the impact it could have.

**Likelihood x Impact = Risk level**

**Likelihood**

Likelihood refers to the potential of a particular risk occurring in your business.

Three levels of likelihood are provided as examples, but you can have as more than three for your business.

- **Very likely**: Almost certain – it will probably occur several times a year
- **Likely**: High probability it will happen once a year
- **Unlikely**: Unlikely but not impossible.

**Impact**

Impact refers to the seriousness of the damage which could occur if the risk happens.

The reporting entity knows its business and is in the best position to know how it would be affected by any impacts. What impacts may affect it and how those impacts would affect it. Some examples of impacts to think about could include:

- How the business would be affected by a financial loss from a crime.
- The risk that a particular transaction may result in a terrorist act and loss of life.
- The risk that a particular transaction may result in funds being used for any of the following: corruption, bribery, tax evasion, drug trafficking, human trafficking, illegal arms trading, terrorism, theft, or fraud.

Note that these do not cover every scenario and are not prescriptive.

Three levels of impact are shown here, but the reporting entity can have as many as necessary for its business:

- **Major**: Severe damage
- **Moderate**: Moderate level of damage
- **Minor**: Minimal damage.

Once the reporting entity assesses the likelihood and impact of each risk, it can then determine the inherent risk level based on these two factors. The following is an example of how a reporting entity can use a risk matrix to determine the inherent risk level posed by customers.

### Risk matrix

You can use a risk matrix to combine the **likelihood** and **impact** to obtain a **risk score (inherent risk level)**. The inherent risk level may be used to aid decision making and help in deciding what action to take.

How the inherent risk score is derived can be seen from the risk matrix shown below. Three levels of risks are shown (Low, Medium and High), but you can have more than three if necessary.

### Risk matrix

| Likelihood/Impact | Minor(1) | Moderate(2) | Major(3) |
|---|---|---|---|
| Very likely(3) | Medium<br>3 | High<br>6 | High<br>9 |
| Likely(2) | Low<br>2 | Medium<br>4 | High<br>6 |
| Unlikely(1) | Low<br>1 | Low<br>2 | Medium<br>3 |

### 5.6.5 Apply controls to manage risks

The response/control to the risk will depend on the level of risk as shown in the table below.

**Response table**

| Risk score | Risk level | Description and response | Residual Risk |
|---|---|---|---|
| 6-9 | High | Risk likely to happen and/or to have serious consequences.<br>Response:<br>Do not allow transaction until risk reduced. | Medium |
| 3-4 | Medium | Possible this could happen and/or have moderate consequences.<br>Response:<br>May go ahead but take steps to reduce risk. | Low |
| 1-2 | Low | Unlikely to happen and/or have minor or negligible consequences.<br>Response:<br>Okay to go ahead. | |

This step is about determining how to manage the risks you have identified and assessed. Managing ML/TF/PF risks involves applying your systems and controls. Examples of risk reduction or controls could be:

i. setting transaction limits for high-risk products (for example limiting the amounts or frequency of transactions)
ii. having a management approval process for higher-risk products or customers
iii. a process to place customers in different risk categories and apply different identification and verification methods
iv. not accepting customers who wish to transact with a high-risk country.

The following table provides an example of how you could record this information.

**Example: Customers**

| Risk | Likelihood | Impact | Risk score | Control/action |
|---|---|---|---|---|

| Risk | Likelihood | Impact | Risk score | Control/action |
|---|---|---|---|---|
| New customer | Likely | Moderate | 2 | Standard ID check<br>ID verification type |
| Customer who brings in large amounts of used notes or small denominations | Likely | Major | 3 | Non-standard ID check<br>ID verification type |
| Customer whose business is registered overseas with no Zambian office | Very likely | Major | 4 | Do not accept as a customer |

It is important to keep in mind that if a customer, transaction or country is identified as high risk it does not necessarily mean that criminal activity is occurring or will occur.

The opposite is also true. Just because a customer or transaction is seen as low risk, this does not mean the customer or transaction is not involved in criminal activity. Your knowledge of your business and common sense should be applied to your risk management process.

### 5.6.7 Monitor and review

Once documented, the reporting entity should develop a method to regularly evaluate whether its AML/CTPF program is working correctly. If not, it needs to work out what needs to be improved and put changes in place. This will help keep its program effective and also meet the requirements of the FIC Act.

Keeping records and regularly doing an evaluation of a reporting entity's risk and AML/CTPF program is essential. Risks change over time, for example, changes to the reporting entity's customer base, its products and services, its business practices and the regulatory requirements.

## 6.0 REPORTING OF MONEY LAUNDERING/ TERRORIST FINANCING/ PROLIFERATION FINANCING RISK ASSESSMENT RESULTS

The results of the ML/TF/PF risk assessment should be presented to senior management and the board and communicated by the Compliance Officer to all business units and the control functions of the institution. The report should clearly indicate proposed action points to be adopted by the institution.

The Institutional ML/TF/PF Risk Assessments that will be developed by the reporting entities should be approved and signed off by the Board of Directors or senior management and be reviewed at such intervals as required by the Board or by changes in the regulatory environment. Reporting entities shall provide to the FIC and/or supervisory authority with a report on the latest results of its MT/TF/PF risk assessment as and when required.

## 7.0 CONCLUSION

Money laundering is a serious economic threat to the country's financial system and can have negative consequences at national, sectoral and institutional level. Non-compliance with AML/CFT regulations can expose the reporting entity to significant regulatory and reputational damage. As such, effective anti-money laundering systems need to be designed to be able to detect and prevent money laundering and the financing of terrorism in financial institutions and DNFBPs. The institutional ML/TF/PF Risk Assessment is one of the tools intended to prevent reporting entities from being exposed to the proceeds of crime, terrorist financing, proliferation financing and other financial crimes.

**ISSUED BY THE FINANCIAL INTELLIGENCE CENTRE**
**MARCH, 2021**