FINANCIAL SERVICES AUTHORITY

SAINT VINCENT & THE GRENADINES

GUIDELINES:

CONDUCTING AML-CFT/CPF INSTITUTIONAL RISK ASSESSMENTS

Issued: January 12, 2023

TABLE OF CONTENTS

TABLE OF ACRONYMS

AML	**Anti- Money Laundering**
BCs	**Business Companies**
CDD	**Customer Due Diligence**
CFT	**Counter-Financing of Terrorism**
CO	**Compliance Officer**
CPF	**Countering Proliferation Financing**
DNFBPs	**Designated Non-Financial Business and Professions**
EDD	**Enhanced Due Diligence**
FATF	**Financial Action Task Force**
FI	**Financial Institution**
FIU	**Financial Intelligence Unit**
FSA	**Financial Services Authority**
ML	**Money Laundering**
NRA	**National Risk Assessment**
NRSPs	**Non-Regulated Service Providers**
PEP	**Politically Exposed Person**
PF	**Proliferation Financing**
RO	**Reporting Officer**
RBA	**Risk Based Assessment/Approach**
SAR	**Suspicious Activities Report**
SDD	**Simplified Due Diligence**
TF	**Terrorist Financing**
UBO	**Ultimate Beneficial Owner**

1.0 Introduction

The Financial Action Task Force (FATF) Recommendation 1 and its Interpretive Note (paragraph 8) as well as the Anti-Money Laundering and Terrorist Financing Regulations (Regulations), 2014 and the Anti-Money Laundering and Terrorist Financing Code, 2017 (the Code) ("the relevant legislation") require financial institutions (FIs)/service providers or Non-Regulated Service Providers/ Designated Non-Financial Businesses and Professions (NRSPs/DNFBPs) to conduct and document a risk assessment of their money laundering (ML)/ terrorist financing (TF) and proliferation (PF) risks. To execute an ML/TF/PF risk assessment, an entity should take appropriate steps to identify and assess the ML/TF/PF risks related to customers, countries or geographic areas, products, services, transactions and delivery channels. Further, in keeping with the requirement of Recommendation 15, FIs are required to identify and assess ML/TF/PF risks that may arise in relation to (a) the development of new products and technologies and new business practices, including delivery mechanisms, and (b) the use of new or developing technologies for both new and existing products. ML/TF/PF risk, like other risks organisations may face, is not static and is evolving. Therefore, FIs and NRSPS are required to ensure that ML/TF/PF risks are continuously reviewed and updated.

The assessment of ML/TF/PF risk is the first step in developing a robust Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) programme. The risk assessment serves to assess the risk of ML/TF/PF a service provider may reasonably expect to face during the course of its business and the establishment of risk profile of its customers. The risk assessment also provides the basis for the implementation of risk-based measures including Customer Due Diligence (CDD), Enhanced Due Diligence (EDD) and Simplified Due Diligence (SDD) measures.

Upon completion of such risk assessment and on the basis of the results therein, a service provider shall document the risk assessment including its findings and the methodology used to conduct same, and accurately develop ML/TF/PF risk mitigating measures, inclusive of policies, controls and procedures that enable it to effectively manage and mitigate the risks that have been identified. When assessing risk, a service provider should consider all the relevant risk factors before determining what is the level of overall risk and the appropriate level of mitigation to be applied.

An adequate system of ML/TF/PF risk management should include:

- ***A risk assessment of ML/TF/PF risks of the business;***
- ***Policies and procedures to control ML/TF/PF risks;***
- ***An organizational structure to execute these risk management controls;***
- ***A process to systematically check and assess the adequacy of the control systems; and***
- ***Independent audit function to test the system.***

2.0 Definitions

- Consequence – the possible outcome or impact of an undesirable event. Which may cause loss and or reputational damage.
- Likelihood – the chance and or frequency of a risk materializing
- Risk – an uncertain event that could influence the achievement of an institution's objectives. Risk is the probability that the actual outcome of an activity will differ from the expected outcome.
- Risk Appetite- the amount of risk a service provider is willing to accept or retain in order to achieve its strategic objectives. It reflects the risk-taking philosophy of the firm and in turn influences the risk culture.
- Risk Management - the discipline by which an institution identifies, assesses, controls, measures and monitors various risks and opportunities for the purpose of achieving its compliance, strategic, operational and financial objectives.
- Risk Monitoring - the continual review and critical observance of an institution's risk management framework to determine any changes to the mitigation strategies employed to further reduce the consequences or impact of the risk.
- Inherent Risk - Inherent risk is the risk which cannot be segregated from a service provider's business activities. It is intrinsic due to the nature of the business performed by the institution.
- Residual Risks - the amount of risk that remains after controls and mitigation strategies have been implemented.

3.0 Purpose

The purpose of this guideline is to primarily assist service providers in evaluating the sources of ML/TF/PF risks and vulnerabilities and to formulate and document their risk assessment and implement risk mitigation measures pursuant to the relevant legislation.

Pursuant to the FATF Recommendations and the relevant legislation, service providers **must undertake** and **document** their **risk assessment and must establish a programme to include measures to manage and mitigate ML/TF/PF risks.**

The risk assessment and programme should reflect a risk-based approach that allows service providers some flexibility in the steps they take when meeting their AML/CFT obligations. A risk-based approach does not prevent a service provider from engaging in transactions/activities or establishing business relationships with higher-risk customers. Rather, it should help them to effectively manage and prioritize their response to ML/TF/PF risks. The examples in this guideline

are suggestions to help service providers meet their obligations under the AML/TF/PF Regulations. They are not exhaustive and are illustrative in nature.

This guideline is for provision of guidance only and cannot be relied on as evidence of complying with the requirements of the relevant legislation.

4.0 Scope of Application

Every service provider regardless of size and complexity, is expected to develop an adequate risk management system for ML and TF. This management system is to ensure that the ML/TF/PF risks are continuously and comprehensively identified, assessed, monitored, managed and mitigated.

This Guideline is not intended to be prescriptive, nor does its broad applicability mean a "one-size-fits-all" approach to conducting an institutional risk assessment. Service providers need to consider the nature, size, scale and scope of their operations and adopt the method of risk assessment that best suits each business as long as it is adequate for the business and tailored to the local context. For example, large service providers may have their own systems and methodology for conducting a risk assessment. However, they should be able to explain and demonstrate to the FSA, the adequacy and effectiveness of procedures, policies and controls stated therein, within the context of Saint Vincent and the Grenadines' (SVG's) AML/CFT requirements. Service providers should submit their risk assessments to the FSA immediately upon completion and annually as updated.

The contents of this Guideline and the examples provided herein are neither intended to, nor shall it be construed as an exhaustive treatment of the subject and the FSA may revise this Guideline by revoking, varying, amending or adding to its content.

5.0 General Requirements

At a minimum, the risk assessment shall:

1. Be documented and approved by the Board;

2. Identify and understand the ML/FT risks your business reasonably expects to face, keeping in mind;
    - The nature, size and complexity of the business;
    - The products and services offered;
    - Delivery channels;
    - Customer types; and
    - Geographical locations.

3. Consider applicable identified threats and vulnerabilities identified in the risk assessment conducted at the national level, including those conducted by supervisors or another competent authority such as the Financial Intelligence Unit (FIU).

4. Enable service providers to determine the level of risk involved in relation to obligations under the *Proceeds of Crime Act 2013*, the *Anti-Money Laundering and Terrorist Financing Regulations, 2014*, the *Anti-Money Laundering and Terrorist Financing (Amendment) Regulations, 2017* and the *Anti-Money Laundering and Terrorist Financing* Code, *2017*.

5. Allow for the preparation of an AML/CFT programme to manage and mitigate the risks identified through the risk assessment.

The risk assessment forms part of a service provider's RBA. It should enable the entity to understand how and to what extent it is vulnerable to ML/TF/PF. It is geared towards assisting the service provider to determine the level of resources that is needed to mitigate the risk. The risk assessment should always be documented, updated and communicated to all relevant persons within the entity including junior and senior management staff. A risk assessment does not need to be complex but should be commensurate with the nature of size of the business activities. The risk assessment should form the basis for the development of policies and procedures to mitigate ML/TF/PF risks, reflecting the risk appetite of the service provider and stating the risk level deemed acceptable. The risk assessment should be regularly reviewed, and updated. Policies, procedures, measures and control to mitigate ML/TF/PF risks should be commensurate with the risk assessment.

5.1 Business Risk Assessment

The first step is to identify and analyze the ML/TF/PF and other integrity risks by means of a business risk assessment. This assessment enables the service provider to comply with (legal) requirements in a risk-based manner. To adequately carry out a business risk assessment, a service provider will conduct and document an assessment of its overall exposure to risks to its organizational structure, its corporate culture, its customers, the jurisdictions with which its customers are connected, its products and services, and how it delivers those products and services. A service provider should analyse those risks that may expose the entity to risks such as ML, TF, but also, corruption, violations of sanctions regulations, and tax evasion. With a tailor-made business risk assessment, the service provider should be able to make informed decisions about the risks that it is willing to take and the control measures that have to be taken.

Risks are not static. Both internal and external factors can cause the risks for a service provider to change. Mergers, acquisitions, the purchase or sale of a business, the adoption of a new technological solution, the introduction of a new product or service, a restructuring or a change of legal structure are some of the events which can affect both the type and extent of the risks to which the service provider could be exposed. In light of any such changes the business risk assessment should be reviewed to consider whether the risks to the entity have changed and to ensure that the controls to mitigate those risks remain effective. Other operational changes, for example, a change in employee numbers or a change to the group policies, can all have an impact upon the resources required to effectively manage ML/TF/PF risks.

Service providers should therefore conduct a business risk assessment at least annually and whenever there are trigger events. Service providers need to consider the possible inherent/gross risks that may arise and the different ways in which they can arise when providing services to clients, but also when the client base changes, or when legal requirements or business strategies change. Service providers must assess in a clear manner whether the existing controls are adequate and effective. If these are not (fully) sufficient, amendments must be made to close these gaps in the controls. When assessing the risks, all relevant employees need to be involved. This means that employees who have direct client contact or handle and assess client documents and transactions, who are aware of all activities and risks, are actively involved. The Board, (senior) management and the AML/CFT Reporting Officer (RO) and AML/CFT Compliance Officer (CO) also have an essential role. The RO and CO have good knowledge of the risks and can guide the process. But management should also have a clear understanding of ML/FT risks. Information about the business risk assessment should be communicated to management in a timely, complete, understandable and accurate manner so that it is equipped to make informed decisions. The risk assessment serves as a steering document for management, on the basis of which management must decide on the actions to be taken.

The business risk assessment should be tailored to the nature and size of the service provider. By considering the nature, scale and complexity of the business, the diversity of the operations (including geographical diversity), the volume and size of transactions, and the degree of risk associated with each area of its operations, the service provider can tailor the risk assessment. Service providers have different risk profiles depending on the types and number of clients and the quantity and type of services that are provided. Service providers with a high-risk profile, for example service providers that mainly onboard and retain clients with a high inherent risk or provide products with a high risk for ML/TF/PF, will also have to devote extra attention to this in the business risk assessment. For example, by developing more risk scenarios, being even more critical about the effectiveness of the control measures, and also to think 'outside the box' about possible scenarios.

5.2 Identification of Risk

In conducting a business risk assessment, a number of steps have to be taken. An important step is drawing up an organization overview: a 'snapshot' of the service provider. This means that over a period of, for example, one or more years, the number and types of clients are analyzed and how often certain transactions have been conducted or certain services provided. In the organization overview, there should be an indication of which countries the clients and the service provider do business and the roles performed by certain employees or third parties. It is important that the service provider collects quantitative data about the entire customer base, products, transactions and services. For this, service providers should consider questions such as:

- What business type are we? Who are we and what do we do?
- How and where do we carry on our business activities?
- Who do we do business with?
- How many and what type of customers do we have?
- Where do our customers reside or do business?
- How are our customers introduced to us?
- Do we have mainly non-face to face contact with customers?
- Do we provide complex or simple services or products?
- Do we have multiple or single premises?
- Do we rely on any third party or introducers to process our business or act on our behalf?
- Is our head office in another jurisdiction?
- Do we have any branches or subsidiaries in other jurisdictions?

The more clients of a certain type there are or the extent to which high risk services or products are provided, the greater the likelihood that a risk manifests itself. Notwithstanding, risks can also

arise with services that are not core business of the service provider. It is important therefore that the service provider collects quantitative data about or has a very good knowledge of the entire client base, its products, transactions and services and its delivery channels.

The essence of a business risk assessment is to map threats and vulnerabilities with regard to each integrity risk, and to assess, by way of risk scenarios, the likelihood that a scenario will occur and what the consequences may be. A risk scenario is a description of how a risk can materialize, or in other words how the service provider can be used for ML/TF/PF or other integrity issues. Risk scenarios describe the threats and vulnerabilities concerning combinations of risk factors such as clients, third parties, employees, delivery channels, countries or services.

Examples of risk scenarios in which a service provider may be confronted with ML/TF/PF or other integrity issues:

A service provider runs a risk of being used for money laundering through clients with ownership structures that include international entities or trusts.

A service provider runs a risk of being used for money laundering through clients whose ultimate control is concealed by the use of nominee shareholders.

A service provider runs a risk of being used for money laundering through loans to customers by unaffiliated third parties.

A service provider runs a risk of being used for corruption or money laundering through clients whose Ultimate Beneficial Owner (UBO) is a Politically Exposed Person (PEP) with unexplained wealth.

A service provider runs a risk of being used to facilitate drug trafficking by facilitating wire-transfers to third parties who are unknown and are involved in drug trafficking activities.

A service provider runs a risk of being used for terrorist financing and proliferation financing (TF and PF) in instances where their clients trade with or has connections to sanctioned countries.

5.3 New Technologies

The risk assessment of a technology does not have to include a highly technical, comprehensive report on the specifications and functionality. The objective of the risk assessment is to evaluate the ML/TF/PF risks and vulnerabilities inherent in the use of the technology and to identify the controls necessary to mitigate and limit the service provider's exposure. It will be necessary that, if the service provider decides to proceed with the adoption or use of a new or developing technology for a new or pre-existing product, the Board/Senior Management/Owner is informed of and approves the risk assessment.

6.0 Factors for Consideration in Identification of Risks

Reporting entities must, at a minimum, assess, the products and services offered; delivery channels; the different types of customers; and geographical locations. The following provides guidance on factors for consideration when assessing these risks, however, service providers should note that these are not exhaustive:

6.1 Nature, Size and Complexity

The size and complexity of the business plays an important role in how susceptible it is for ML/TF/PF. For example, businesses that accept cash from the public are at more risk than those that only accept cheques or bank transfers. A business that conducts complex transactions across international jurisdictions could offer greater opportunities to money launderers and terrorist financiers than a purely domestic business. Service providers should consider the ability of its customers to use the business to spread their funds across numerous products in order to avoid detection.

With the use of internal data, this will help service providers work out what parts of their business are vulnerable to ML/TF/PF activity. For instance, a service provider may have identified a higher-risk product, but without knowing how many of those products have been provided to customers, and where they are domiciled, this will result in a flawed assessment of risk.

6.2 Transaction, Products and Services Offered

Certain products and services offered by service providers may pose a higher risk of ML/TF/PF depending on the nature of the specific product or service offered. Such products and services may facilitate a higher degree of anonymity, or involve the handling of high volumes of currency or currency equivalents.

Hence, when assessing products and services risk, service providers should be mindful of the complexity, value/size of the product, service or transaction and the level of transparency that the product offers:

Complexity of the product, service or transaction – The extent to which a transaction is complex and if it involves multiple parties or multiple jurisdictions has to be assessed. For example, in the case of certain trade finance transactions, are transactions straightforward; are regular payments made into a pension fund. Additionally, service providers must consider whether the product or service allows payments from third parties or accept overpayments where this is not normally expected. Where third party payments are expected, consideration has to be given to whether the identity of the third party is known; whether the product and service are funded exclusively by fund transfers from the customer's own account at another financial institution that is subject to AML/CFT standards or whether it allows movement of funds in a rapid or complex manner, or

across borders.

Value/size of the product, service, transaction - High value products or services increase the risk of money laundering and terrorist financing occurring. High value products or services offer those seeking to undertake ML and TF the opportunity to move illicit funds in large amounts with limited exposure. In the same way, service providers have to know the products or services that may be low value but high frequency. The ability to hide amongst other transactions and conduct frequent transactions is a key factor for those seeking to undertake ML or TF.

The level of transparency the product offers - An AML/CFT risk assessment should always incorporate whether any products offer anonymity or opaque ownership. Opaque ownership provides those seeking to undertake money laundering with an ability to remain unknown to authorities. This provides options for laundering large amounts, sometimes on behalf of others, making it a valuable avenue for ongoing abuse.

For the risk assessment, the service provider will describe all products and services that it provides and make an estimate of the likelihood that customers will misuse that product for ML/TF/PF, and the impact thereof to form its risk profile. Additionally, prior to introducing new products, service providers should assess the potential ML risks associated with same, to ensure that the appropriate mitigating mechanism is in place.

Some of these products and services are listed below, however, the list is not exhaustive:

- Electronic funds payment services — prepaid access (e.g., prepaid cards), domestic and international funds transfers, payable upon proper identification transactions, third-party payment processors, remittance activity, and automated teller machines (ATM);
- Electronic banking;
- Private banking (domestic and international);
- Trust and asset management services;
- Monetary instruments;
- Foreign correspondent accounts (e.g., international funds transfers, payable through accounts(PTA), and drafts);
- Night safe;
- Services provided to third-party payment processors or senders;
- Foreign exchange;
- Special use or concentration accounts (e.g., intra-day, suspense accounts);
- Lending activities, particularly loans secured by cash collateral and marketable securities;

- Non-deposit account services (e.g., non-deposit investment products and insurance); and
- Safe deposit.

When considering whether the products and services your business offers could be exploitedfor ML/TF/PF purposes, you can consider the following:

- Does the product/service allow for anonymity?
- Does the product/service disguise or conceal the identity of the beneficial owner?
- Does the product/service disguise or conceal the source of wealth or funds of your customer?
- Does the product/service allow payments to third parties?
- Does the product/service commonly involve receipt or payment in cash?
- Has the product/service been identified in the National Risk Assessment (NRA), FIU or FSA guidance material, or any Sector Risk Assessments as presenting a higher ML/TF/PF risk?
- Does the product/service allow for the movement of funds across borders?
- Does the product/service enable significant volumes of transactions to occur rapidly?
- Does the product/service allow the customer to engage in transactions with minimal oversight by the service provider?
- Does the product/service have an especially high transaction or investment value?
- Does the product/service have unusual complexity?
- Does the product/service require government verification of customer eligibility?

Note: Many other factors can contribute to the ML/TF/PF risk of the service provider's products and services. Itwill be the service provider's responsibility to identify those factors as part of the risk assessment.

6.3 Delivery Channels

The way your business on-boards your customers and delivers your products and services affects its vulnerability to ML/TF/PF. When identifying the risk associated with delivery channels, service providers should consider the risk factors related to the extent that the business relationship is conducted on a non-face to face basis, any introducers or intermediaries the service provider uses and the nature of their relationship to the service provider.

How the service provider delivers products or services is a key component to measuring risk. This includes not only at the time of client onboarding but also throughout the client's relationship with the business. Should a client use the service of the service provider for the

placement stage of the laundering cycle, without detection, it becomes more difficult to detect ongoing activity as unusual or suspicious. Hence, it is important to have very good controlsfor client identity and verification, as well as understanding the nature and purpose of the client's relationship with the business. Additionally, the use of intermediaries may result in the client's identity, beneficial owner or effective controller not being transparent to the business. Service providers have to ensure that written agreements are in place which clearly describe each party's responsibilities. Furthermore, there must be procedures in place to monitor compliance of the intermediary at periodic intervals.

In assessing the delivery channel risks, service providers should assess the different delivery channels in the business and how many of these channels are used by product and service. This will provide a more accurate presentation of the risks faced per delivery channel.

For example, the service provider can assess whether:

- The customer is physically present for identification purposes. If they are not,
  - Whether the service provider uses reliable forms of customer due diligence measures; and
  - The extent that the service provider has taken steps to prevent impersonation or identity fraud.
- Products/services are provided via the internet;
- The service provider has indirect relationships with customers (via intermediaries, pooled accounts, etc.);
- Products/services are provided by means of agents or intermediaries; and
- Products/services are provided to overseas jurisdictions.

6.4 Customer Types

Although any type of account is potentially vulnerable to ML/TF/PF, by the nature of their business, occupation, or anticipated transaction activity, certain customers and entities may pose specific risks. It is essential that service providers exercise judgment when assessing customer types, as opposed to treating or defining all members of a specific category of customer as posing the same level of risk.

Some categories of customers pose a higher risk of ML/TF/PF than others, especially when combined with higher-risk products/services and jurisdictions. Service providers need to determine the breakdown of their customer base, assessing where the customers originate or the types of transactions they are performing, in line with how they use the products/services of the institution, etc. At the end of the assessment, service providers should be able to show which of their customers are High, Medium or Low risk.

Some examples of specific customers and entities are detailed below:

- Foreign financial institutions, including banks and foreign money services providers (e.g., currency exchanges, and money transmitters).
- Non-bank financial institutions (e.g., money services businesses; casinos; brokers/dealers in securities; and dealers in precious metals, stones, or jewels).
- Individuals who are or have been entrusted with prominent public function and their family members and close associates (politically exposed persons (PEP), be they domestic or foreign[1].
- Foreign corporations and domestic business entities, particularly international corporations (such as shell companies and business companies (BCs) located in higher-risk geographic locations.
- Cash-intensive businesses (e.g., convenience stores, restaurants, retail stores).
- Non-governmental organizations and charities (foreign and domestic).
- Professional service providers (e.g., attorneys, accountants, or real estate brokers).
- Virtual currency exchanges.

The service provider needs to ask the following questions when assessing both its new and existing customers:

- Are they a trust or other legal person?
- Have the beneficial owners been identified?
- Are they specified in the AML/CFT Act and Regulations as requiring enhanced due diligence?
- Are they involved in occasional or one-off activities/transactions above a certain threshold?
- Do they use complex business structures that offer no apparent financial benefits?
- Are they a PEP?
- Are they a cash-intensive business?
- Are they involved in businesses associated with high levels of corruption?
- Do they have an unexplained or hard to verify source of wealth and/or source of funds?
- Do they conduct business through, or are they introduced by, gatekeepers such as accountants, lawyers, or other professionals?
- Are they a non-profit organisation?
- Have they been identified in the NRA, FIU or FSA guidance material or Sector Risk Assessment as presenting a higher ML/TF/PF risk?

Note: This list is not exhaustive, and many other factors can contribute to customer ML/TF/PF

[1] For further guidance on this component see the Politically Exposed Person Guidance on the FIU's website https://www.svgfiu.com/index.php/publications/guidance/205-politically-exposed-person-pep-guidance

risk. As with the products and services it is the service provider's responsibility to identify those factors as part of the risk assessment.

6.5 Geographical Locations

It is important to understand that the risks associated with a country are wider than having insufficient AML/CFT measures in place. Identifying geographic locations that may pose a higher risk is essential to a service provider's AML/CFT compliance program. A service provider's business is exposed to geographical risk through a variety of ways including where clients (including beneficial owners) are domiciled or hold citizenship, where transactions or activities are originating from or being sent to and for clients that operate as businesses, where their business operations stretch, including jurisdictions representing their customer base.

Service providers should understand and evaluate the specific risks associated with doing business in, opening accounts for customers from, or facilitating transactions involving certain geographic locations. However, geographic risk alone does not necessarily determine a customer's or transaction's risk level. Service providers have to ensure that they understand the links between their clients and the different jurisdictions they operate in, transact with or originate from, so that an effective assessment of the risk can be undertaken.

There is no general characterization to determine which particular countries or geographic locations can be categorised as low or high risk. The factors which may determine if a specific country or geographic location is more vulnerable to ML/TF/PF, may include different criteria. Notwithstanding, higher-risk geographic locations can be either international or domestic, and depend on the effectiveness of the AML/CFT regime employed, the level of predicate offences in the jurisdiction, terrorism financing risks, transparency etc. On the other hand, international higher-risk geographic locations generally include:

- Countries subject to sanctions, embargoes or comparative restrictive measures issued, by organisations or countries such as the United Nations, European Union or the United States.
- Jurisdictions or countries monitored for deficiencies in their regimes to combat ML/TF/PFby international entities.
- Offshore financial centres (OFC).
- Other countries identified by the service provider as higher-risk because of its prior experiences or other factors (e.g., legal considerations, or allegations of official corruption).
- Domestic higher-risk geographic locations.

To assist in the determination of a country's geographic risk, different sources of information

can be used. These include:

- FATF list of high-risk and non-cooperative jurisdictions;
- FATF mutual evaluation reports;
- European Union AML and tax blacklists;
- Basel AML Index;
- United Nations Office on Drugs and Crime (UNODC) reports;
- Transparency International Corruption Perceptions Index;
- Know Your Country reports;
- Trusted and independent media sources; and
- United Nations sanctions, embargoes or similar measures.

An analysis of the above factors should lead to the service provider being able to identify the geographic breakdown associated with its customers/transactions and to put in place adequate monitoring systems and measures to address the risks.

7.0 Obligations of the Board and Senior Management vis-à-vis Risk Assessments

The Board and Senior Management are ultimately responsible for determining the risk appetite, setting the tone at the top in instituting measures to combat AML/CFT, including risk-based measures.

Board and Senior management's leadership abilities and commitment to the prevention of ML/TF/PF are important aspects when implementing a risk-based approach to combat ML/TF/PF risks. The Board and Senior Management should encourage regulatory compliance and ensure that employees abide with internal procedures, policies, practices and processes aimed at risk mitigation and control.

Given the responsibilities of the Board and Senior Management and considering that AML/CFT risk management forms an integral part of the risk and compliance management framework of reporting entities, the Board should remain informed of potential AML/CFT risks. The Board should have a clear understanding of ML/TF/PF risks with timely information about ML/TF/PF risk assessment communicated in a complete, understandable and accurate manner (reports should be made on an ongoing basis, in a timely and accurate manner) so that it is equipped to make informed decisions.

Responsibilities of the Board vis-à-vis the institutional risk assessment include:

- approving and overseeing appropriate policies for risk management;
- determining the service provider's risk appetite;
- establishing internal controls; and
- being actively engaged with the Senior Management of the service provider.

It is the responsibility of the Board to ensure that Senior Management is taking necessary steps to identify, measure, monitor and manage the AML/CFT risks, including implementing strategies to mitigate these risks. Senior Management is in turn responsible for establishing and communicating a strong awareness of, and need for effective internal controls, policies and procedures within the organization.

Service providers should have in place internal controls which include appropriate governance arrangements where responsibility for AML/CFT is clearly allocated, and are implemented in accordance with the applicable local legislation. In particular, there is a requirement for the Board /Senior Management to approve and oversee the policies for risk, risk management and compliance.

Explicit responsibility should be allocated by the Board/Senior Management, effectively taking into consideration the governance structure of the service provider, ensuring that policies and procedures are managed effectively. The Board/Senior Management should appoint an appropriately qualified CO and a RO, to have overall responsibility for the AML/CFT function with the stature and the necessary authority, experience and independence within the service provider, such that issues raised by these senior officers receive the necessary attention from the Board, Senior Management and business lines.

7.1 Risk Appetite

The determination of the service provider's risk appetite is an important element in carrying out the business risk assessment, setting out the amount of ML/TF/PF risk it is prepared to accept in pursuing its strategic objectives. The Board/senior management is responsible for setting the service provider's risk appetite, together with the overall attitude of the service provider to risk-taking. The primary goal of the risk appetite is to define the amount of risk that the service provider is willing to accept in the pursuit of its objectives, as well as outlining the boundaries of its risk taking, beyond which the service provider is not prepared to accept risk.

Identifying the amount of such risk that it is willing to take on is an integral part of the design and implementation of appropriate and effective policies, procedures and controls to manage and mitigate risk. The service provider's risk appetite includes a qualitative statement (for example, detailing those categories of customers or countries that are deemed to pose too great a risk) as well as quantitative statements on the service provider's risk limits, the maximum level of risk that can be accepted.

In developing a risk appetite, the following questions can be posed:

- What kind of clients do we want to accept?
- What kind of clients do we not want to accept?
- Which jurisdictions are we avoiding?
- Which jurisdictions are not acceptable?
- Which percentage of our client base can be high risk?
- Which core services do we want to provide?
- What risks will we treat on a case-by-case basis?

8.0 Assessing ML/TF/PF Risk

This phase involves a thorough and informed assessment of the nature, sources, likelihood, and consequences of risks to the service provider's business. In determining the level of ML/TF/PF risk associated with a business relationship or transaction, service providers should take a holistic view of the ML/TF/PF risk factors they have identified.

8.1 Assessing Likelihood and Consequence of Risk

One way to determine the level of risk is to determine how **likely** the risk is and cross-reference that with the **consequence** of that risk (see the example of a risk matrix below).

Using likelihood ratings and consequence ratings can provide a more comprehensive understanding of risk and a robust framework to help arrive at a final risk rating. These ratings, in combination with structured professional opinion and experience, will assist in applying the appropriate risk management measures as detailed in the service provider's programme.

For example, a service provider may have identified that one of its products as vulnerable to ML/TF/PF and it assesses that the likelihood of this product being used in ML/TF/PF activity is *highly probable*.The service provider judges the impact of the identified risk happening in terms of financial loss and assess the consequence as *moderate*.

Cross-referencing *highly probable* with *moderate* in the risk matrix below results in a final inherent risk rating of *medium-high*. The service provider's programme should then address this *medium-high* risk with appropriate control measures. The service provider will need to undertake this exercise with each of its identified risks. The risk matrix below is provided as an illustrative example only.

Likelihood scale	5 Almost certain	11	16	20	23	25
	4 Highly probable	7	12	17	21	24
	3 Possible	4	8	13	18	22
	2 Unlikely	2	5	9	14	19
	1 Improbable	1	3	6	10	15
		1 Minimal	2 Minor	3 Moderate	4 Significant	5 Severe
	Consequence scale					
Risk rating	Low	Medium		Medium-high	High	

8.2 Assigning Risk Weights

Another way to determine the level of risk is to assign weights to risk factors. When weighting risk factors, service providers should make an informed judgment about the relevance of different risk factors in the context of a business relationship or transaction.

The weight given to each of these factors is likely to vary from product to product and customer to customer (or category of customer) and from one service provider to another. When weighting risk factors, service providers should ensure that:

- Weighting is not unduly influenced by just one factor;
- Economic or profit considerations do not influence the risk rating;
- Weighting does not lead to a situation where it is impossible for any business relationship to be classified as high risk;
- Situations identified by national legislation or the sectoral supervisor as always presenting a high money laundering risk cannot be over-ruled by the service provider's weighting; and
- Service providers are able to override any automatically generated risk scores where necessary. The rationale for the decision to override such scores should be governed and documented appropriately.

Service providers which do not develop automated IT systems in-house to allocate overall risk scores to categorise business relationships or transactions, should ensure that they understand how the system works and how it combines, or weighs, risk factors to achieve an overall risk score. Service providers should be able to satisfy the supervisory authority that it understands the system used for assessing ML/TF/PF risks and that the system reflects its understanding of these risks.

9.0 Managing ML/TF/PF Risks

Critical to the risk management process is the development and implementation of AML/CFT/CPF policies, controls, and procedures commensurate with the identified risk of the service provider. In addition, there should be equivalent reporting and accountability structures to enhance the systems implemented to manage the identified risk.

This risk management process includes in short, the following tasks and processes.

1. identifying and analyzing ML/TF/PF and other integrity risks;
2. the management of risks through policies, procedures and systems;
3. monitoring and checking that policies and procedures are actually being implemented and systems are working properly;
4. assessing whether the risks are adequately and effectively controlled;
5. reviewing policy and procedures where necessary;
6. informing employees about risks and revised policies and procedures.

A risk-based approach allows for the Board/senior management of a service provider to implement policies, procedures and controls tailored to its operations and risk posture. It also helps to produce a more cost-effective system of risk management and promotes the prioritization of AML/CFT efforts.

9.1.1 Assessing Effectiveness of Control Measures

The effectiveness of the controls per risk scenario also has to be assessed. For this, among others, audit reports, information from compliance monitoring and incident reports can be used. It is important that a realistic assessment is made whether the existing measures are being effectively applied and implemented.

In assessing the existing level of controls, the following criteria can be used:

1. The control is fully operational and fully effective.
2. The control could be improved in certain areas, but works adequately and is effective
3. Substantial improvement is necessary, but the control has some effect.
4. There is no control, or the control has no effect.

9.1.2 Determining Additional Measures

By comparing the inherent risks with the control measures, service providers can determine the net risks and gaps in the existing control measures. On the basis of this, service providers will assess which additional measures have to be taken. A business risk assessment provides insight into the extent to which risk can actually occur and if the risk must be further reduced to an acceptable level. Service providers must also consider whether the (gross and net) risks fall within the risk appetite. The risk analysis provides service providers and its management with clear insight into the risks that need to be controlled and which (additional) measures need to be taken.

With a tailor-made business risk assessment, service providers assess whether there are gaps in the controls. If a risk has a higher likelihood of materializing, this must also be reflected in (amendments of) the policies and the procedures and the knowledge and awareness of employees. The identified risks will have to be incorporated in various processes of the service provider, such as the customer acceptance, transaction monitoring, reporting of unusual transactions or incidents. If the risk analysis shows that there is a (too) high net risk for certain types of clients, then the client acceptance process, the review process as well as the transaction monitoring on these clients will have to be enhanced. Service providers must have appropriate mechanisms to document and provide risk assessment information to the supervisor, which is the FSA.

9.2 Risk Mitigation

Service providers should develop and implement policies and procedures to mitigate ML/TF/PF risks they have identified. CDD processes should be designed to assist the service provider to understand their customers and why they require the service. The initial stage of CDD should be designed to assist the service provider to assess its ML/TF/PF risks associated with the transaction or business relationship, determine the level of CDD to be applied and deter persons from establishing relationships or conducting transactions to conduct illicit activities. Based on all the information obtained in the context of the application of CDD, the service provider should be able to establish a risk profile. The establishment of the risk profile of the customer should determine, inter alia, the level and type of on-going monitoring to apply, whether to proceed with the transaction or enter into a business relationship and terminate the business relationship.

Risk profiles can be applied at the individual customer level or where groups of customers display similar characteristics (for example, clients of similar income range or conducting similar types of transactions (for example, pensioners).

The application of the RBA to CDD is useful as it may support financial inclusion objectives by providing more flexible application of CDD measures to certain financial products or customers who might otherwise face challenges to meet service providers' CDD requirements. However,

financial exclusion by itself is not an indicator of low ML/TF/PF risk and service providers will need to make an informed decision, based on the holistic ML/TF/PF risk assessment, whether exemptions or SDD measures are applicable.

9.3 Internal Controls

Once the inherent risks have been identified and assessed, internal controls must be evaluated to determine how effectively they offset the overall risks. Controls are programmes, policies or activities put in place by the service provider to protect against the materialisation of a ML risk, or to ensure that potential risks are promptly identified. Adequate internal controls are a prerequisite for the effective implementation of policies and measures to mitigate ML/TF/PF risks. Internal controls include appropriate governance arrangements where responsibilities are clearly assigned, controls to monitor the integrity of staff, and controls to test the overall effectiveness of the service providers' policies and processes to identify, assess and monitor risk.

Many of the same controls apply to various activities undertaken within the service provider and will be executed by both the Front Office staff (*1st line of defense*) and Compliance function (*2nd line of defense*).

The controls in place are evaluated for their effectiveness in mitigating the inherent money laundering risk and to determine the residual risk rating. AML controls are usually assessed across the following control categories:

- AML Corporate Governance; Management Oversight and Accountability;
- Adequacy of policies and procedures;
- Effectiveness of Customer Due Diligence ("CDD"), Know Your Client ("KYC") measures, Enhanced Due Diligence (EDD) measures;
- Previous Other Risk Assessments (local and enterprise-wide);
- Management Information/Reporting;
- Record Keeping and Retention;
- Independence and effectiveness of designated AML Compliance Officer/Unit;
- Effectiveness of detection, analysis and reporting of SARs;
- Monitoring and Controls;
- Sanction screening systems
- Effectiveness of training activities;
- Independent Testing and Oversight (including recent Internal Audit or Other MaterialFindings); and
- Other Controls.

The successful implementation and effective operation of the RBA to AML/CFT is dependent on strong senior management leadership and oversight of the development and implementation of the RBA across the service provider. The role of senior management includes:

i. Promoting compliance as a core value of the institution. Senior management, together with the Board of Directors (where applicable), are responsible for setting up robust risk management and controls adapted to the stated, sound risk-taking policies;
ii. Implementing adequate mechanisms of internal communication related to actual or potential ML/TF/PF risks faced by the institution;
iii. Deciding on the measures needed to mitigate ML/TF/PF risks identified and on the extent of residual risk the service provider is prepared to accept; and
iv. Adequately resourcing the service provider's Compliance Department.

Service providers should take steps to be satisfied that their AML/CFT policies and controls are adhered to and effective. Therefore, the controls should be monitored on an ongoing basis by the service provider's Compliance Officer. In addition, the adequacy of and compliance with the service provider's AML/CFT controls should be reviewed as a first step by the service provider's internal auditor (*3rd line of defense*) or, by an independent auditor.

10.0 Updating of ML/TF/PF Risk Assessment

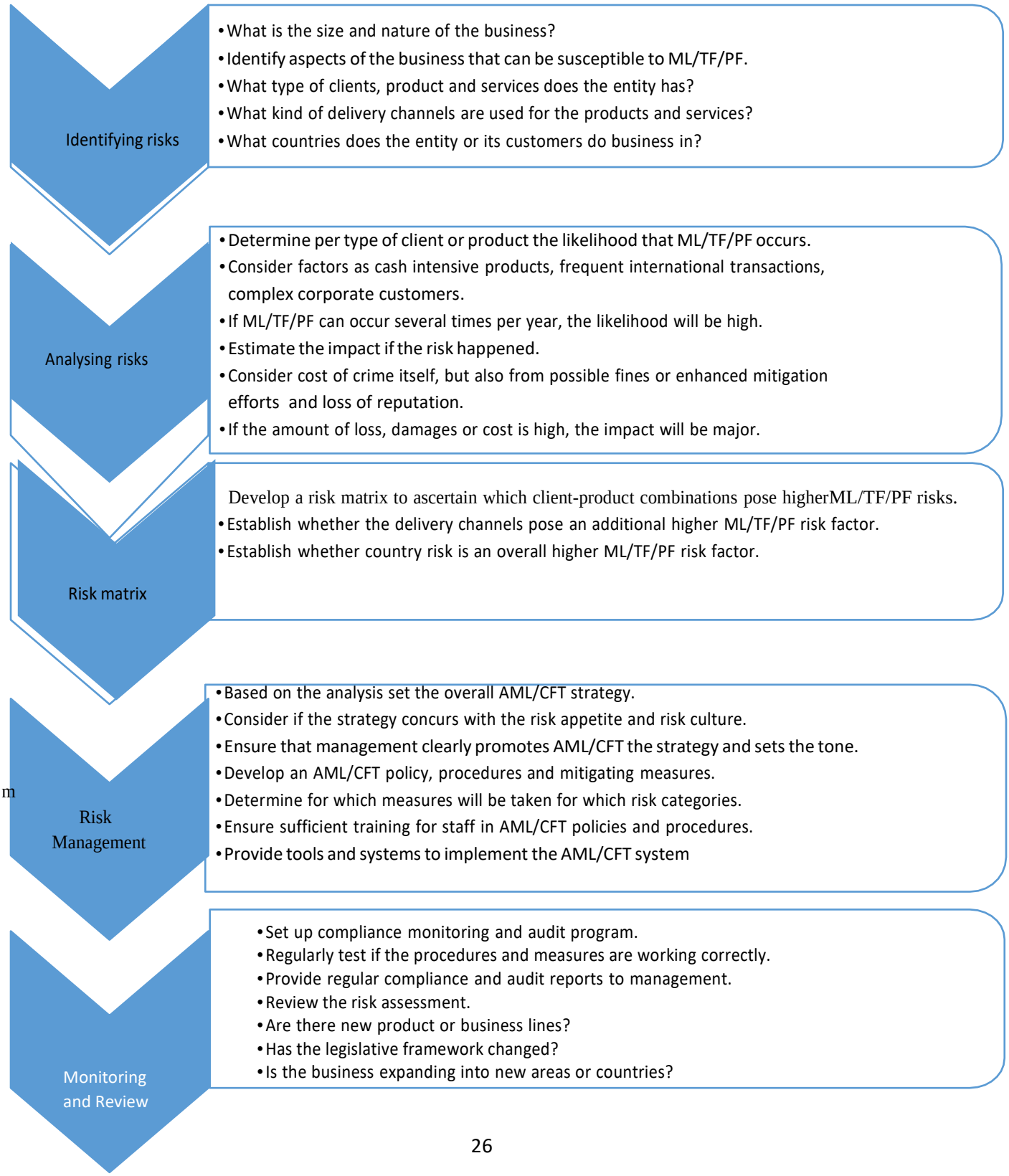
As part of the risk assessment, service providers should describe the process for updating the assessment. Service providers should put in place systems and controls to keep their assessments of the ML/TF/PF risks associated with their business, and with their individual business relationships under review to ensure that their assessment of ML/TF/PF risks remains upto date and relevant.

As previously stated, the risk assessment should be submitted to the FSA by September 30 every year. However, service providers will have to ensure that changing, new or emerging risks are included in risk assessments and that resources allocated to mitigate the risk remains proportionate to the risk level. Where a service provider is aware that a new risk has emerged, or an existing one has increased or decreased, this should be reflected in the risk assessment, as soon as possible.

As part of new risks, these can include trigger events such as, the emergence of new technologies; a new customer base; new services or products; new ML/TF/PF risks as determined by the FATF, supervisory authority or the FIU; or updated laws or regulations.

Additionally, carefully recording issues throughout the relevant period that could have an impact on risk assessments, such as internal suspicious transaction reports, compliance failures and intelligence from front line staff, can assist in the updating of risk assessments. Finally, as mentioned before, when updating risk assessments, service providers should always bear in mind the applicable identified threats and vulnerabilities from the NRA and any sectoral assessments, to ensure that ML/TF/PF risk inherent to them is understood at the national/country level and same is reflected in the risk assessment conducted at institutional level.

APPENDIX 1: STEPS TO BE TAKEN IN CONDUCTING A ML/TF/PF RISK ASSESSMENT



APPENDIX 2: AML CFT CPF RISK ASSESSMENT REPORT TEMPLATE

BUSINESS NAME
AML/CFT RISK ASSESSMENT REPORT
MONTH 20XX

TABLE OF CONTENTS

1. Introduction

This AML/CFT Risk Assessment Report (the "Report") is issued in accordance with paragraph 23 of the *Anti-Money Laundering and Terrorist Financing Code, 2017* ("the Code") and the AML/CFT Institutional Risk Assessment Guidelines issued by the Financial Services Authority ("FSA").

1.1 Overview of Business Activities

Provide a brief overview of the Company's profile, including background information such as business structure, services/products offered, general overview of the categories/types of customers to which services/products are provided, geographic location of customers and any other appropriate information)

1.2 Purpose of Risk Assessment

To effectively prevent money laundering and combat the financing of terrorism, an assessment mechanism that adopts Risk-based Approach is established to carry out regular overall assessment of money laundering and terrorist financing (ML/TF/PF)risks so as to grasp effectively the distribution and controls of ML/TF/PF risks.

1.3 Period and Frequency of Risk Assessment

The Company conducts an overall ML/TF/PF risk assessment at least once every year.

The assessment period for which this Report is applicable **insert date* to *insert date*.

2. ML/TF/PF Risk Assessment Process

The ML/TF/PF risk assessment methodology was conducted in accordance with the following process:

a) Identifying the inherent risks through a review of customer risk factors for the past one year and assessing its likelihood and consequences for the forthcoming year; and

b) Evaluating the risk controls programmes.

For effective risk analysis, this process was documented on a risk chart as follows:

Risk Type	Risk Description	Likelihood (L)	Consequence (C)	Risk Score (L x C)	Risk Mitigation Strategy
Nature, size and complexity of business risk	The business transfers funds to international jurisdictions that may lead to MT/TF activities	**5**- Almost Certain	**5**-Severe	**25**	Keep, update and communicate a list of high-risk jurisdictions for ML/TF

2.1 Risk Factors and Risk Weights

The Company analysed the ML/TF/PF risks facing the Company in **five/six* risk factors category, with percentage weighting assigned as follows:

Risk Factor	% Weight Assigned
Nature, size and complexity of business risk	*x %*
Customer Risks	*x %*
Product/Service Risks	*x %*
Geographic Risks	*x %*
Transaction and Delivery Channels Risks	*x %*
*Others (if any)	*x %*

3. Overall Risk Assessment Result

Based on the analysis of inherent risks, the Company's overall vulnerability to ML/TF/PFis rated as ****LOW/MEDIUM/HIGH.***

3.1 Inherent Risk Statistics

(a) Nature, size and complexity of business risk

**Provide an overview of the size and complexity of your business relative to the market being operated in, for example, asset size, premium income etc.*

(b) Customer Risks

**Provide detailed summary and statistics of the categories/types of customers to whichservices/products are provided. You may also insert*

statistics based on the Risk Assessment results in the below table for the period being assessed.

Customer Type	% Customers
e.g., Individual Customers	
e.g., Non-Individual Customers	
e.g., Politically Exposed Customers	
e.g., Foreign Customers	

(c) Product/Service Risks

**Provide detailed summary of the general products/services offered to customers. You may also provide information on the percentage of customers that has used the different services for the period being assessed.*

(d) Geographic Risks

**Provide detailed summary of the geographic locations of customers for the period being assessed, including the percentage of customers from the specified location.*

(e) Transaction and Delivery Channel Risk

**Provide description of the manner in which products/services are delivered to customers and the manner in which transactions are conducted for the period being assessed. This includes the number/percentage of customers which are obtained face-to- face, non-face-to-face or through intermediaries. For transactions, this should outline the manner in which transactions are conducted, that is, whether transactions are conducted through banking facilities, cash or a combination of both.*

3.2 Inherent Risk Assessment Result

Following the analysis of inherent risks, the key ML/TF/PF risks of the Company are classified in the following four risk category:

(a) Customer Risk

**Brief overview of what is the main risk posed by your customers, including its likelihood of it occurring and the risk rating assign to the customer risk factor*

(b) Product/Service Risk

**Brief overview of what is the main risk posed by the services/products, including its likelihood of it occurring and the risk rating assign to the product/service risk factor*

(c) Geographic Risk

**Brief overview of what is the main risk posed by the geographic risk of the customer,its likelihood of it occurring and including the risk rating assign to the geographic riskfactor*

(d) Transaction and Delivery Channel Risk

**Brief overview of what is the main risk posed by the transaction and delivery channelsused, its likelihood of it occurring and including the risk rating assign to the transactionand delivery channel risk factor.*

4. Risk Control Measures

4.1 Risk Management Policy

On the basis of risk perception, controls commensurate with the size and risk level of the Company shall be adopted, which are prioritized corresponding to the assessed riskacross the four risk factors category, namely:

(a) Customer Risk

(b) Product/Service Risk

(c) Geographic Risk

(d) Transaction and Delivery Channel Risk

4.2 Action Plan of Risk Management

In the face of inherent ML/TF/PF risks in each risk factors category, the Company, in linewith the requirements of the Proceeds of Crime Act, 2013 and guidelines issued by the FSA, and in considering the Company's nature of business, nature and profile of its customer, adoptsthe following AML/CFT controls to mitigate the inherent risks which have been identified:

- Verification of customer identity
- Record keeping
- Reporting of cash transactions above the threshold to the FIU

- ❖ Reporting of suspicious activities and/or transactions to the FIU
- ❖ Appointment of a compliance officer at the management level to take chargeof AML/CFT compliance matters
- ❖ Screening procedures to screen persons before recruitment and on an ongoing basis
- ❖ Ongoing employee training plan
- ❖ Regular review of procedures implemented

**controls listed above to be selected based on the risks identified*

5. Conclusion

Based on the combined analysis of inherent risks and risk control measures, the Company's overall risk level is determined to be ****LOW/MEDIUM/HIGH***