Anti-Money Laundering and Countering the Financing of Terrorism Institutional Risk Assessment Guidelines

February 2021

Table of Contents

Document Information

Document Owner	Financial Intelligence Unit
Creation Date	February 2021
Version	V1.0

Document Review History

Date	**Version**	**Document Amendments/Insertion**
February 15, 2021	V1.0	Document Creation

List of Acronyms

AML	Anti-Money Laundering
AML/CFT Act	Anti-Money Laundering and Countering the Financing of Terrorism Act, 2020
CDD	Customer Due Diligence
DNFBPs	Designated Non-Financial Businesses and Professions
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
LEA	Law Enforcement Agencies
ML	Money Laundering
NPOs	Non-Profit Organisations
NRA	National Risk Assessment
PEP	Politically Exposed Persons
STRs	Suspicious Transaction Reports
TF	Terrorist Financing

1. Introduction

1.1. These guidelines are issued by the Financial Intelligence Unit ("FIU"), pursuant to section 57 (2) of the Anti-Money Laundering and Countering the Financing of Terrorism Act 2020,("AML/CFT Act"), with the aim to assist reporting entities in ensuring compliance with Section 32 (1) of the Anti-Money Laundering and Countering the Financing Terrorism Act 2020 ("AML/CFT Act") which requires every reporting entity to take the necessary measures to identify, assess, understand and monitor its risk of money Laundering ("ML") and terrorist financing ("TF") activities and to take appropriate measures to mitigate the risks identified.

1.2. The extent to which a reporting entity understands its risks is a crucial element for the development and implementation of appropriate and adequate measures, which are commensurate to the nature and size of its business, for the proper management and mitigation of those risks. Therefore, the AML/CFT programme implemented must address the risks identified by the reporting entity.

1.3. As the Supervisory Authority for Designated Non-Financial Businesses and Professions ("DNFBPs") specified under Part C of the First schedule (except entities at serial number 7and 8) of the AML/CFT Act, the Financial Intelligence Unit ("FIU") is responsible for ensuring compliance by those reporting entities with provisions of the AML/CFT Act.

1.4. The *Anti-Money Laundering and Countering the Financing of Terrorism Institutional Risk Assessment Guidelines* is issued by the FIU, pursuant to section 57 (2) of the AML/CFT Act, to provide guidance to its reporting entities on how to conduct and document their AML/CFT risk assessment in line with the requirements of the AML/CFT Act. The guidance provided in these guidelines will be subjected to ongoing reviews, and may be updated to reflect any new changes in the ML/TF trends and patterns, both in the domestic and international landscape that may pose a risk to the reporting entities.

2. Scope of the Guidelines

2.1. These guidelines are being issued to reporting entities specified under Part C (except entities at serial numbers 7 and 8) of the First Schedule of the AML/CFT Act.

2.2. The guidelines herein outline the minimum standards set out by the AML/CFT Act which should be adopted by the reporting entity to develop an effective ML/TF risk assessment framework and must be read in conjunction with the AML/CFT Act and Regulations; and any other directions or guidelines issued by the FIU. Please note that it is not a replacement for and does not supersede the legislation and regulations that reporting entities should comply with, as part of their regulatory obligations.

2.3. It is not mandatory for the reporting entity to adopt the procedures and templates provided for by these guidelines when conducting its risk assessment as long as the reporting entity's risk assessment is reliable, relevant to their business and comprehensible to all parties involved. As such, the reporting entity should be able to effectively demonstrate its compliance with the regulatory requirements.

3. Risk Assessment Obligation of the Reporting Entity

3.1. Pursuant to Section 32 (1) of the AML/CFT Act, every reporting entity shall take measures to identify, assess, understand and monitor its risks of ML and TF activities and take appropriate measures to mitigate the risks identified. In accordance with Section 32 (5) of the AML/CFT Act the outcome of the risk assessment is required to be documented and made available to the FIU, as the Supervisory Authority and Law Enforcement Agencies ("LEAs"), upon request.

3.2. When conducting its risk assessment, reporting entity must in line with Section 32 (2) of the AML/CFT Act take into account amongst other things the following factors;

- the profile of its customers;
- the geographic area in which it conducts business;

- the product(s) that it deals in;
- the service(s) that it provides to its customers/clients;
- the means by which such products or services are delivered to its customers/clients;
- the transactions that it conducts;
- customer due diligence carried out by third parties; and
- the technological developments in identifying such risks.

3.3. In addition, reporting entity must take into consideration information obtained from relevant sources such as:

- the outcome of any risk assessment carried out at national level (the National Risk Assessment ("NRA")) or sectoral level (Sector Risk Assessments);
- guidance documents issued by the FIU; and
- trends and typology reports issued by the FIU

3.4. In accordance with Section 32 (6) of the AML/CFT Act, a reporting entity which fails or neglects to take reasonable measures to identify, assess and monitor the money laundering and terrorist financing activities, commits an offence, and is liable on conviction, to a fine not exceeding SCR 400,000.

4. The Risk Assessment Process

4.1. As part of the risk assessment process, a reporting entity must consider all relevant inherent ML/TF risks factors that may increase their business' vulnerability to being abused by money launderers and for terrorist financing activities.

4.2. A simple risk assessment process to assess the business' ML/TF risk exposure and vulnerability as depicted in *(Fig. 1* hereunder) consist of:

i) Identifying the ML/TF risks (inherent risk);
ii) Assessing the ML/TF risks;

iii) Implementation and Evaluation of the AML/CFT internal controls;

iv) Documentation of the Risk Assessment results; and

v) Reviewing and updating the Risk Assessment on an on-going basis

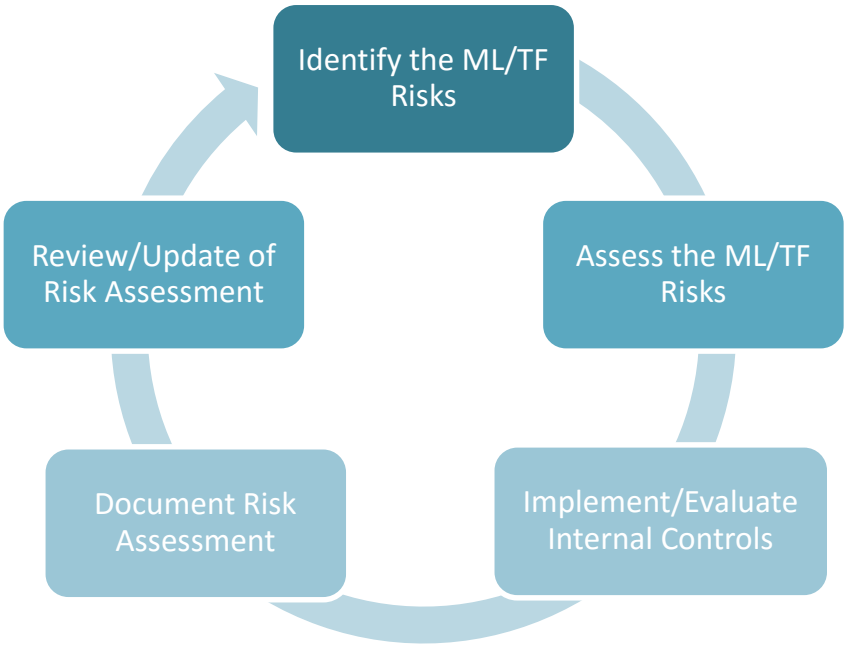

Fig. 1. Risk Assessment Process

4.3. A comprehensive risk assessment also includes the assessment of the residual risks i.e., the risks after the AML/CFT internal controls have been implemented. It assists in determining how effective the controls implemented are at mitigating the identified risks. However, this is not a required component of the risk assessment. Should reporting entities wish to assess its residual risk as part of its risk assessment, it should ensure that it is able to demonstrate how it arrived at the residual risk ratings.

5. Identifying the ML/TF Risks

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

5.2. Generally, the size and complexity of the reporting entity's nature of business plays a role in how vulnerable it is to ML/TF risk. For example, a business with a large customer base is less likely to know its customers personally and may offer a greater degree of anonymity than a business with a small customer base.

5.3. In conducting its risk assessment to identify those areas of its business that may be susceptible to ML/TF risk, the reporting entity should consider the following risk factors:

i) Customer Risks – the type of customers they conduct business with;
ii) Product/Service Risks – the type of products and/or services provided to its customers;
iii) Geographic Risks – the geographical location of its customers;
iv) Transaction and Delivery Channels Risks – the manner in which products and/or services are delivered to and transactions are conducted with its customers;
v) Other Factors – any other risks factors as identified by the reporting entity

5.4. The factors described below and description provided as per ***Appendix I*** are not exhaustive and reporting entities may consider other pertinent risk factors applicable to the nature, size and complexity of its business. It is to be noted that **not** all risk factors outlined will be relevant or applicable to the business.

5.4.1. Customer Risks

The reporting entity should understand the nature and the level of risks that their

customers may bring into their business, as certain category of customers may pose a higher ML/TF risk than others. In establishing the customer risks, the following criteria but not limited to, may be considered:

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

5.4.2. Product/Service Risks

Reporting entities should assess the potential risks arising from the products and services that they offer to their customers. Certain products and services, by their nature, may present high vulnerability to ML/TF and thus may be exploited for ML/TF purposes. In assessing the risks of the products/services provided, it is recommended that the following is considered:

- whether the product/service allows for anonymity;
- whether the product/service allow the identity of the beneficial owner to be obscured;
- whether the product/service disguise or conceal the source of wealth or funds of the customer;
- whether the product/service commonly involve the receipt or payment in cash;
- whether the product/service have a high transaction or investment value; and
- whether the product/service has been identified in the NRA, FIU Guidance documents or Trends & Typology Reports as presenting a higher ML/TF risk.

5.4.3. Geographic Risks

Geographical risk may arise with respect to the location or nationality of a customer or the origin and the destination of transactions conducted by the customer. This is in view that different geographic location poses different level of AML/CFT risks, based on the prevailing factors in that particular jurisdiction.

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

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

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

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

5.4.4 Transaction and Delivery Channel Risks

The manner in which customers are on-boarded and services/products are provided to customers (delivery channels) and the manner in which transactions are conducted affects the business' vulnerability to ML/TF. For example, customers on-boarded non-face-to-face or through intermediaries presents a higher vulnerability to ML/TF by nature due to the challenges that may occur in the verification of the customer's identity.

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

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

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

5.4.5. Any other Factors

Reporting entities may also assess other factors, which may apply to the nature of their business, which does not fall in the categories outlined above. It is important to note that there may be a particular feature about a business that can make it more attractive to individuals who want to carry out ML/TF activities.

6. Assessing the Money Laundering Risks

6.1. Once the different risks have been identified, the reporting entity should determine the level of those risks within its business. The methodology of the risk assessment provided herein is one of a lower complexity, and is limited to only considering the likelihood of the ML/TF event occurring. Reporting entities wishing to undertake a more in-depth risk assessment, may also assess the impact (consequences) that the ML/TF event may have on its business.

6.2. The ML/TF risk assessment should consider each risk factor (event) that has been identified and consideration of the likelihood that the event may occur based on the business' experience based on historical/present data and publicly available information such as NRA, Sectoral Risk Assessments and Trends and Typology reports issued by the FIU.

6.3. A likelihood score is assigned to each risk factor based on the Likelihood Scores Index (***Table 1 – Likelihood Scores Index***) and the respective risk rating is assigned (***Table 2 – Risk Classification***).

Table 1 – Likelihood Scores Index

LIKELIHOOD SCORES INDEX

- 0 – No likelihood of the event occurring
- 1 – Rare, occurs only in exceptional circumstances
- 2 – Unlikely, may occur at some point
- 3 – Possible, likely that the event will occur at some point
- 4 – Likely, the event is likely to occur in most cases
- 5 – Very Likely, the occurrence of the event is considered as normal

Table 2 – Risk Classification

RISK CLASSIFICATION	**LOW**	**MEDIUM**	**HIGH**
RISK SCORE	0 – 1	2 – 3	4 – 5
INDICATION	Low probability that the risk is present	Probable that the risk is present	High probability that the risk is present

6.4. Reporting entities may use the **AML/CFT Institutional Risk Assessment Template** to assess their institutional risk. Please note that it is not mandatory for reporting entities to use the template or the risk model outlined as long has the reporting entity is able to effectively demonstrate its risk assessment methodology and that it has taken reasonable measures to identify and assess its risks.

7. Implementing and Evaluating the AML/CFT Internal Controls

7.1. Once the reporting entity has identified its ML/TF risk exposure, internal controls must be implemented and evaluated to determine how effectively they offset the identified risks. Controls are programmes, policies or activities put in place by reporting entities to prevent their businesses from being used to facilitate ML /TF, or to ensure that potential risks are promptly identified and mitigated accordingly.

7.2. There are a number of controls which can be implemented to mitigate the identified risks which are a regulatory requirement as per the AML/CFT Act, and as such, are also used to maintain compliance with the AML/CFT regulatory requirements.

Example 1

Risk: Large cash transactions conducted without proof of source of funds
Controls: i) Introduce a large cash declaration form
ii) Perform daily or weekly checks on large cash transactions
iii) Provide staff with training on where risk of ML arises

Example 2

Risk: High volume of clients originating from high-risk countries

Controls: Conduct enhanced due diligence on such clients such as screening using World Check, conducting adverse media searches, requesting for proof of source of fund and source of wealth etc.

7.3. As part of the risk assessment process, the internal controls implemented should be periodically reviewed and tested for effectiveness to verify whether any amendments are required in light of any emerging risks or change in existing risks identified by the reporting entity.

7.4. Stated hereunder are examples of control measures controls which can be implemented, but is not limited to by reporting entity to mitigate identified risk

i) Implementation of AML/CFT Programme

The risk assessment should enable you to prepare a comprehensive AML/CFT programme and meet your obligations under the AML/CFT Act, including procedures for the application of customer due diligence, monitoring of customer transactions and reporting of suspicious activities. Although the policies and procedures implemented must meet the minimum requirements prescribed by the legislations, it must also be commensurate with the level and type of risks faced by the reporting entity.

ii) Compliance Officer Function

The Compliance Officer has the overarching responsibility to ensure that the AML/CFT measures established by the reporting entity is being implemented effectively. Whilst assessing its risks, reporting entities are able to obtain a broad view of its customer profiles, the volume and type of businesses (services/products), volume and type of transactions routing through it and the potential ML/TF risks to the business. As the business' level of complexity, size and risk increases, the risk assessment should help

in determining whether the resources being allocated to its compliance function is sufficient to continuously meet its regulatory obligations (e, g. should the Compliance Officer continue discharging additional duties other than the compliance function, should additional staff be employed in the compliance function, etc…).

iii) Applying appropriate Customer Due Diligence ("CDD") measures

Policies and procedures can be implemented to determine the level of CDD required for a particular category(ies) of customer, including PEPs based on the extent of the risks being identified. For example, an individual customer whose transaction method is solely through the use of banking facilities may pose a lower ML/TF risk compared to a non-face-face customer originating from a high-risk jurisdiction. As such, the lower risk customer may be subjected to a simplified due diligence process, while the high-risk customer may be subjected to an enhanced due diligence ("EDD") process.

Regulation 15 and Regulation 16 of the AML/ CFT Regulations outlines the measures which are required to be undertaken in the application of simplified and enhanced customer due diligence requirements.

iv) Effective mechanism to monitor transactions and Reporting of Suspicious Transactions

The risk assessment will assist you in determining the triggers, red flags or scenarios which will require more in-depth scrutiny or additional information from a customer. Staff (where applicable) should be provided with adequate awareness on policies, procedures and risk identification to enable them to identify the triggers and red flags, and as a subsequent, allow the effective implementation of the established policies and procedures. This will also improve the quality of monitoring and determination of whether an activity or a transaction may be deemed as suspicious based on the understanding of its customers and reported to the FIU.

8. Documenting the Risk Assessment Results

8.1. In accordance with Section 32 (5) of the AML/CFT Act, the outcome of the risk assessment conducted by the reporting entity is required to be documented, and made available to the FIU, as the Supervisory Authority and to LEAs upon request.

8.2. The results of the risk assessment and any measures undertaken by the reporting entity to mitigate the identified risks should be consolidated within a comprehensive report and communicated to the Company's Directors, Partners or Senior Management (as applicable) to assist them in making informed decisions on the strategic direction of the company.

8.3. To assist reporting entities in documenting their risk assessment, the FIU has devised an **AML/CFT Risk Assessment Report Template** to be used by Reporting Entities under its supervisory purview. Please note that it is not mandatory for reporting entities to use the template as is, and adjustments may be made to best suit the needs of the reporting entity, dependent on its nature, size and complexity of its business.

8.4. Once documented, the reporting entity should ensure that:

- the risk assessment is approved by Senior Management Officials such as the Directors, Partners or Owners of the Business;
- policies and procedures established to mitigate the identified risks are implemented effectively by the business and its staff; and
- ensure that all directors, partners, managers and employees (as the case may be) are adequately informed and trained on the relevant policies and procedures implemented.

9. Review and Update of the Risk Assessment

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

9.2. As such, to ensure that the reporting entity's understanding of its risks remains current and up to date, reporting entities should ensure that the ML/TF risk assessment is performed at least on an annual basis to ensure that any changes within the company's business model and strategy is taken into consideration within the risk assessment. This includes changes in:

- the type or categories of customers which the reporting entity provides services/products to;
- the type of services or products being offered to customers;
- the manner in which services and products are provided (i.e. delivery channels) to customers;
- the transaction methods used by customers; and
- new or emerging risks identified in the National Risk Assessment or through Trends & Typology reports published by the FIU, that may significantly change the risk profile of reporting entities.

Appendix I: Description of Risk Factors

The factors described below are not exhaustive and reporting entities may consider other pertinent risk factors as applicable to their business. It is to be noted that **not** all risk factors outlined will be relevant or applicable to the business.

A. Nature, size and complexity of Business

Risk Factors	Notes
Size of business may mask suspicious activity	The larger your business is, the higher the risk that suspicious activities and transactions may be undetected during the ordinary course of the business. If you are a large business, you may use corporate structure diagrams to help you identify areas of your business that could benefit from increased levels of attention.
The complexity of business makes AML/CFT measures difficult to implement	Greater complexity decreases the transparency of business transactions and activities, increases ML/TF vulnerability and may reduce the effectiveness of AML/CFT measures.
Size of business makes it difficult to implement AML/CFT measures	Large organisations may have difficulty tailoring their AML/CFT measures to meet AML/CFT requirements. Increased size (due to large number of staff) may also result in reduced adequacy and effectiveness of AML/CFT measures.
Nature of your business activities and transactions are recognised as being vulnerable to ML/TF risks	The NRA, relevant Sectoral Risk Assessments, Trends and Typology Reports issued by the FIU, and other supervisory guidance identifies the nature of your business or activities/transactions associated with it as being vulnerable to ML/TF risks.

B. Type of Customers generally dealt with

Risk Factors	**Notes**
Customers and their ownership structure are complex structures	Legal persons with complex and non-transparent structures may hide and disguise beneficial ownership and mask ML/TF activities. Furthermore, customers may establish legal entities in multi-jurisdictional structures to hide the true ownership and control of assets held overseas. Organisational structure diagrams may help you identify beneficial ownership and effective control.
Customers' occupations or nature of business are high risk by nature	Some occupations can have a greater vulnerability to ML/TF. E.g., Cash intensive business, dealers in high-value goods, gatekeeper occupations.
Customers reside in or are citizens of a high-risk jurisdiction	*Refer to Geographic Risks*
Customers are Politically exposed persons	PEP customers may mean greater vulnerability to ML/TF. By nature of positions they hold, PEPs may be considered high-risk through all stages of the ML/TF process, as they can use their positions to influence individuals and institutions and facilitate the movement of funds. Their privileged position (access to state funds and decision-making) heightens ML/TF risks. They may also seek to obscure their financial position using their relatives or close associates.
Customers have other potential ML/TF risks	Other possible risk factors that may be considered are:

	• Customers have been the subject of previous Suspicious Transaction Reports ("STRs") submitted by the company • Customers are the subject of adverse media. N.B. As adverse media may be explained, it is not necessary result in a higher ML/TF risk

C. Products and services offered

Risk Factors	**Notes**
Products/services offered are identified as presenting heightened ML/TF risks	The NRA, relevant Sectoral Risk Assessments, Trends and Typology Reports issued by the FIU, and other supervisory guidance identifies the products/services offered as being vulnerable to ML/TF risks.
Products/services operate using commission-based remuneration	A conflict of interest between effective AML/CFT measures and commercial gain may lead to AML/CFT measures being ignored or reduced in order to gain/maintain business.
Products/services provided support the pooling of funds and investments (e.g. a trust account or client account)?	This can disguise the beneficial ownership of funds. It can enable criminals to place money within the financial system with fewer questions being asked because of the perceived respectability and legitimacy of the source of funds. It can also act as the link between different ML/TF techniques, such as purchasing real estate.
Products/services target foreign-based (offshore) customers	Having customers offshore may expose your business to ML/TF risks that are beyond your control, especially in connection with countries with weak AML/CFT regimes, high levels of corruption and bribery and organised crime.

D. Geographic Locations

Risk Factors	Notes
Business has dealings with or customers in countries that have a weak or ineffective AML/CFT measures	Consider variables such as lesser AML/CFT provisions, weak regulations and law enforcements. Please consult the Mutual Evaluations conducted by the FATF and other AML/CFT publications such as the Basel AML Index, for identification of countries/jurisdictions with AML/CFT deficiencies.
Business has dealings with or customers in countries that have generally high ML/TF risks	Factors such as whether the countries/jurisdictions have a cash intensive economy, whether it is a source of or renowned for illicit activities (organised crimes or drug-related crimes), or whether it has an unstable or weak government and countries identified by credible sources as providing funding for or otherwise supporting terrorist activities.
Business has dealings with or customers in countries that are subjected to sanctions	Consider whether customer is from or is a resident of a country or jurisdiction which is subjected to sanctions. This includes whether the customer themselves appears on any sanctions list e.g. UNSCR 1267, UNSCR 1373

E. Methods of Delivery and Transactions

Risk Factor	Notes
Methods of delivery used for products/services provide for anonymity	Anonymity is highly sought after by criminal elements to facilitate ML/TF. A major part of your AML/CFT

	measures will be focused on removing anonymity and increasing transparency.
Products/services may be obtained through the use of intermediaries	This may result in the customer's identity, beneficial owner or effective controller not being transparent to the reporting entity.
Products/services may be obtained through minimized face-to-face contact with the customer	Less face-to-face interaction with a customer increases vulnerability to ML/TF activity.
Products/services may be obtained by a third party	This may result in your customer's identity, beneficial owner or effective controller not being transparent, which increases ML/TF risk.
Business accepts payments to/from third parties or non-customers	This can disguise the beneficial ownership or effective control of funds. The presence of multiple intermediaries and agents can hide and disguise beneficial ownership.
Business accepts high-value payments through cash transactions	Cash payments may obscure the origins of the source of the funds. Cash-intensive businesses are attractive to criminals as it allows for illicit funds to be mingled with legitimate sources of funds.
Business permits partial payments and accepts structured payments in cash	Criminals may take advantage of partial/structured payments below reporting thresholds so as to avoid detection or raising a red flag.