Financial Intelligence Centre
Republic of Namibia

PO Box 2882
Windhoek
Namibia

Phone: + 264 61 283 5286
Fax: + 264 61 283 5918
Helpdesk@fic.na

GUIDANCE NOTE NO. 16 OF 2023

GUIDANCE ON RISK ASSESSMENTS AND ML/TF/PF INDICATORS

LENDING INSTITUTIONS AS PER ITEM 6 OF FIA SCHEDULE 1 AND OTHER FINANCIAL INSTITUTIONS AVAILING LENDING SERVICES

First Issued: 06 July 2023

TABLE OF CONTENTS

DEFINITIONS AND ABBREVIATIONS

"Accountable Institution (AI)" means a person or entity listed in Schedule 1 of the Act;

"Business relationship" means an arrangement between a client and an accountable or reporting institution for the purpose of concluding transactions on a regular basis;

"CDD" means Customer Due Diligence;

"Client and Customer" have their ordinary meaning and are used interchangeably herein;

"Customer Due Diligence" (CDD) means a process which involves establishing the identity of a client, the identity of the client's beneficial owners in respect of legal persons and monitoring all transactions of the client against the client's profile;

"Enhanced Due Diligence" (EDD) means doing more than the conventional simplified due diligence or the basic CDD measures mentioned above and includes, amongst others, taking measures as prescribed by the Centre to identify, as far as reasonably possible, the source of wealth, funds and any other assets of the client or beneficial owners whose activities may pose a risk of ML, TF or PF;

"Establish Identity" means a two-tier process consisting of *ascertainment or collecting* of certain identification information, and *verification* of some of the information against reliable documentation or information;

"FATF" means the Financial Action Task Force;

"FIA" refers to the Financial Intelligence Act, 2012 (Act No. 13 of 2012);

"FIC" means the Financial Intelligence Centre;

"ML" means Money Laundering;

"PEPs" means Political Exposed Persons (See FIC Guidance Note 01 of 2019);

“PF” means proliferation financing;

“Records” means any material on which information is recorded or marked and which is capable of being read or understood by a person, or by an electronic system or other device;

“Regulations” refer to the FIA Regulations unless otherwise specified;

“RBA” refers to the Risk Based Approach. An approach for managing risks based on prioritization of such risks as per the occurrence/frequency/probability and potential impacts/consequences of each identified risk;

“SAR” refers to a suspicious activity report submitted to the FIC in terms of sections 33 (1) & (2) of the Act;

“Shell company” means an incorporated company with no independent operations, significant assets, ongoing business activities or employees;

“Shelf company” means an incorporated company with inactive shareholders, directors, and secretary, which has been left dormant for a longer period even if a customer relationship has already been established;

“STR” refers to a suspicious transaction report submitted to the FIC in terms of sections 33 (1) & (2) of the FIA;

“TF” means Terrorist Financing;

“Transaction” means a transaction concluded between a client and an accountable or reporting institution in accordance with the type of business carried on by that institution, and includes attempted transactions.

1. BACKGROUND

This document avails sectoral guidance on conducting risk assessments and indicators of common Money Laundering (ML), Terrorism Financing (TF) and Proliferation Financing (PF) activities.

This Guidance Note is issued in terms of Section 9(1)(h) of the Financial Intelligence Act, 2012 (The FIA). It is the first set of two sectoral guidance notes for institutions availing lending services. The guidance herein speaks to how Lending Institutions can conduct risk assessments while Guidance Note 17 of 2023 highlights implementation of risk based control measures. Both guidance notes apply to all Lending Institutions listed in Item 6 of Schedule 1 of the FIA and other financial institutions offering loans such as banks. In this context, as far as their lending services are concerned, they are all collectively referred to as Lending Institutions.

It is common cause that services offered by Lending Institutions have been abused for ML domestically. Internationally, there are trends and typologies which suggest abuse to advance TF/PF activities. To help mitigate ML/TF/PF risks, the Financial Intelligence Centre (FIC) issues this Guidance to help Lending Institutions implement and enhance their internal Anti-Money Laundering, Combatting the Financing of Terrorism and Proliferation (AML/CFT/CPF) measures.

2. COMMENCEMENT

This Guidance Note comes into effect on **07 July 2023**.

3. SCOPE OF SERVICES DESIGNATED IN THE FIA

In terms of item 6 of Schedule 1 of the FIA, a person or entity that carries on the business of lending, including but not limited to the following:

a) The Agricultural Bank of Namibia established in terms of the Agricultural Bank of Namibia Act, 2003 (Act No.5 of 2003);

b) The Development Bank of Namibia established in terms of the Development Bank of Namibia Act, 2002 (Act 8 of 2002); and

c) The National Housing Enterprise established in terms of the National Housing Enterprise Act, 1993 (Act No.5 of 1993).

This document provides guidance related to identifying and mitigating risks within lending services as mentioned above and other types of lending services offered by different financial institutions such as banks and microlending institutions.

4. DEFINING MONEY LAUNDERING

4.1 The ML Process

A. Placement

Involves placing the proceeds of crime in the financial system. *For example, a business obtains a loan and then uses proceeds of crime (e.g from its shareholders, directors, associates etc) to repay such a loan.*

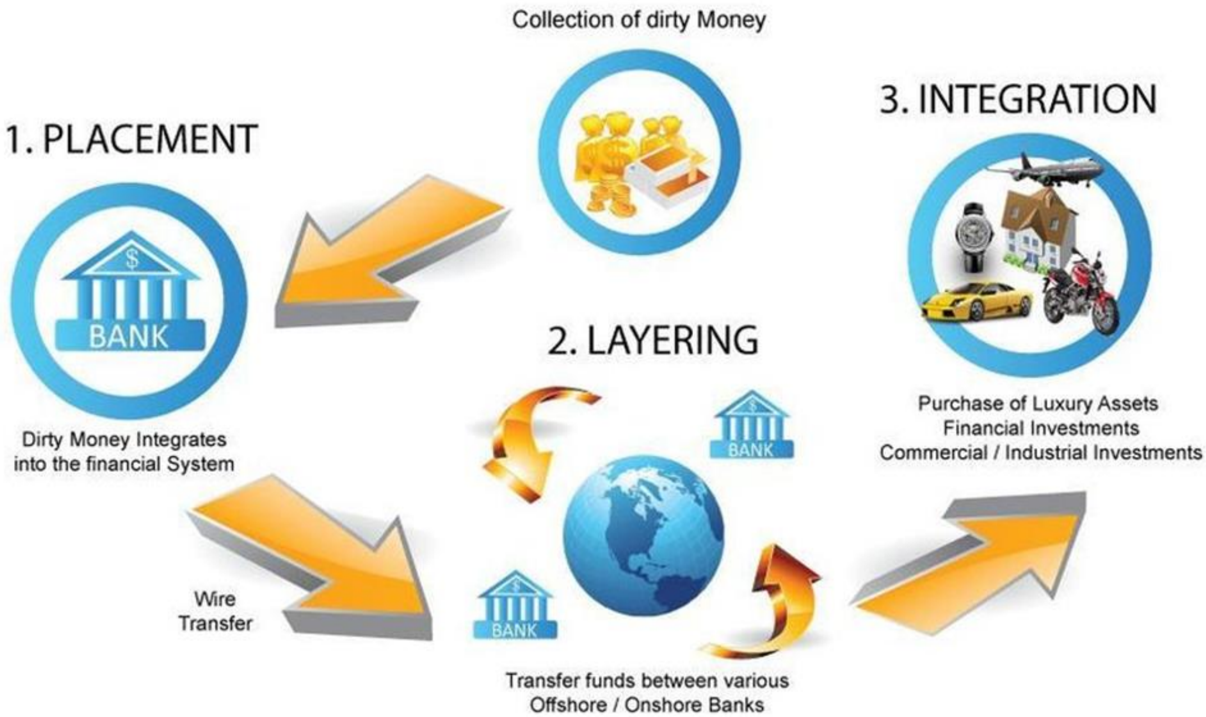
B. Layering

Involves converting the proceeds of crime into another form and creating complex layers of financial transactions to disguise the audit trail and the source and ownership of funds. The aim is usually to create as much distance as possible between the illicit activity/criminal and the illegal proceeds. *For example, Assets or properties bought with proceeds of crime are later sold and proceeds from such sale are presented or used as if such are from legitimate origins. The loans which were initially legally obtained could have been invested in properties or other financial assets for example. Such investments would now appear legitimate as the source of funds could be cited as loans.*

C. Integration

Usually the last stage of the ML process. Integration is at times similar to, or part of the layering process. The aim is to place the laundered proceeds back in the financial system under a veil of legitimacy. *The example given in B above includes a combination of both layering and integration when assets are bought with legitimate loans and the loan is settled with proceeds from illicit activities.*

Below is a diagram of the three layers of ML.



Lending Institutions, as part of their risk assessment process, should assess the ML/TF/PF vulnerabilities and high-risk factors associated with each of their clients applying for or having received loans/mortgage from same. The risk assessment section herein avails indicators of potential high risks. Such should be duly considered for combatting ML, TF and PF.

4.2 ML Vulnerabilities in Lending Institutions

The lending industry is vulnerable to various financial crimes that can threaten the integrity of the financial system. Financial crimes are illicit activities that involve the use of financial systems to launder money or finance criminal activities. The lending industry is particularly susceptible to the following financial crime risks[1]:

a. ***Money laundering:*** *ML is the process of disguising the proceeds of criminal activity as legitimate funds. Criminals often use loans and other financial services to move money and make it appear as if it comes from a legitimate source. Lending Institutions are vulnerable to ML risks if they fail to identify the true source of funds or the intended use of the loan. Below are the most common methods of ML with loans or mortgages:*
    - *Lump sum cash or additional funds are added to the expected periodic repayments; and*
    - *In some cases, criminals would take out loans and after a while use proceeds from their (or their associates') illicit activities to settle such loans in a short period of time. They would have the benefit of having obtained 'clean" money from the loans initially obtained.*

b. ***Fraudulent loan applications:*** *Fraudulent loan applications occur when a borrower provides false information to obtain a loan. This can include falsifying employment records, credit scores, or other financial information. Fraudulent loan applications can be used to launder money, finance criminal activities, or commit other financial crimes;*

c. ***Insider fraud:*** *Insider fraud occurs when an employee of a lender abuses their position to commit fraud. Insider fraud can include embezzlement, ML and other forms of financial crimes. Lending Institutions can be vulnerable to insider fraud risks if they fail to implement effective internal controls and fraud detection*

---

[1] Source: https://sanctionscanner.com/blog/aml-compliance-guide-for-lenders-351#:~:text=Criminals%20often%20use%20loans%20and%20other%20financial%20services,funds%20or%20the%20intended%20use%20of%20the%20loan

measures. Proceeds from employee's fraudulent activities can often result in ML and the lending services would have been the source of such predicate offence; and

d. ***Third-party risks:*** *Lending Institutions often work with third-party service providers, such as credit reporting agencies, loan brokers, and other intermediaries. Lending Institutions can be vulnerable to financial crime risks if their third-party service providers engage in illicit activities, such as ML, fraud, or TF.*

5. TERRORISM FINANCING (TF) RISKS IN LENDING INSTITUTIONS

TF is the process of providing financial or other forms of support to terrorist groups. Lending Institutions can be vulnerable to TF risks if they fail to identify the true source of funds or the intended use of the loan. If persons who are sympathetic to terrorist organisations are directors or members in an entity awarded a loan, the risk of TF is escalated. With natural persons accorded loans, it is also accepted that if they are associated with terrorist groups, the TF risk is enhanced. (See below section on TF risks)

5.1 Nature/Sources of TF funds

As mentioned herein, the characteristics of TF can make it difficult to detect/identify. The methods used to monitor ML can also be used for TF, as the movement of TF funds often relies on similar methods (control vulnerabilities or shortcomings) used for ML. Internationally, TF processes are considered to typically involve the following three stages:

a. *Raising funds* (through donations, legitimate wages, selling items, criminal activity);
b. *Transferring funds* (to a terrorist network, to a neighbouring country for later pick up, to an organisational hub or cell); and
c. *Using funds* (to purchase weapons or bomb-making equipment, for logistics, for compensation to families, for covering living expenses etc).

Funds that are used in TF may be derived from either criminal activity or may be from legitimate sources, and the nature of the funding sources may vary according to the type of terrorist organisation. Funds from loans can be directed to terrorist activities. Where funds are derived from criminal activity, the traditional monitoring mechanisms that are used to identify ML (as explained in this Guidance) may be appropriate for detecting potential TF, though the activity, which may be indicative of suspicion, may not be readily identified as or connected to TF or terrorism.

Risks associated with TF are highly dynamic. As such, Lending Institutions need to ensure that their prevention and combatting measures are current, regularly reviewed, updated and flexible to evolving risks. It is important to maintain preventative and combatting awareness as well as effective transaction monitoring systems that incorporate dynamic TF risks, along the more static risks associated with ML.

5.2 Helpfulness of ML Controls for TF

There are both similarities and differences in the application of the RBA to TF and ML. They both require a process for identifying and assessing risk. However, the characteristics of TF make its detection and the implementation of mitigation strategies challenging due to considerations such as the relatively low value of transactions involved in TF, or the fact that funds can be derived from legitimate as well as illicit sources.

As mentioned in section 5.3 below, Namibia has not observed potential TF exposure within the Lending Institutions sector. This does not however mean the sector is not vulnerable to such abuse. Availing of loans to legal persons and trusts, given their exposure to foreign clients, some of whom may hail from or have ties to terrorist organizations, sympathisers or high-risk countries, remains inherently[2] an avenue which can expose the sector to TF risks. For example, it could only take a sanctioned persons'

[2] Inherent risks refer to the level of (original) risks prior to the implementation of controls to reduce the likelihood and impact of such risks.

presence in the management or ownership of a loanee company not detected for our country to be guilty of advancing TF.

5.3 Sectoral TF Risk Levels

Within the AML/CFT/CPF space, risk is an aggregate of vulnerabilities and threats. This is an essential guide in appreciating why ML is significantly more prominent than TF with lending services.

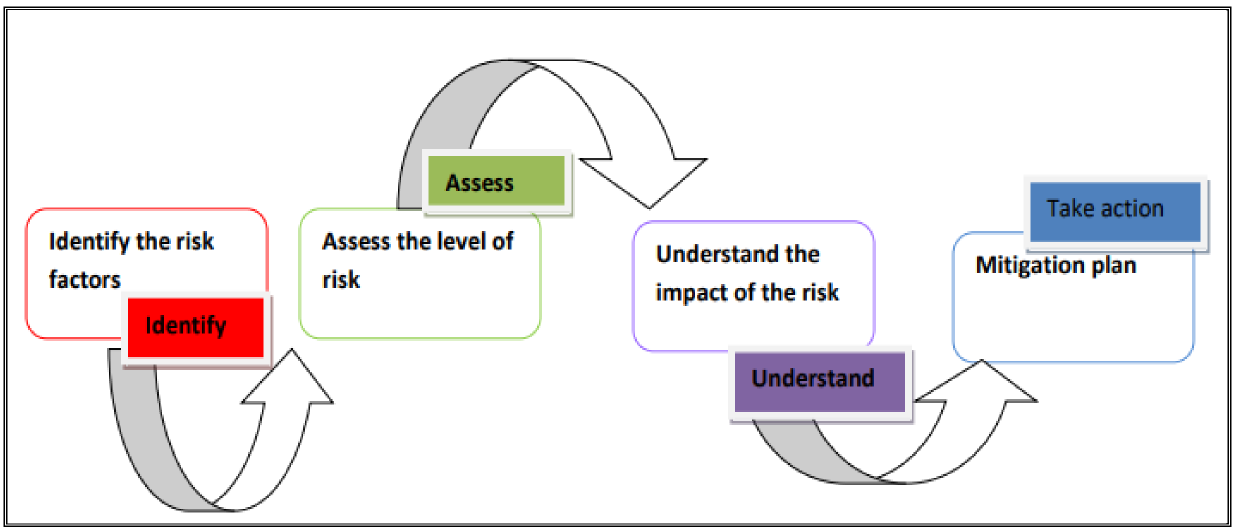
In Namibia, the TF threats are generally low for Lending services, as per 2020 National Risk Assessment (NRA) outcomes. No TF threats (cases or activities to date) were linked to, or associated to lending services. There are no observations, as per the 2023 NRA update to suggest increased threat levels in lending services. Internationally, lending institutions are not commonly known for abuse to advance TF although there are a few examples and typologies showing same. While the 2012 NRA, 2017/18 update and 2020 NRA rightly suggest that ML threats and overall risks are more frequent and prominent, TF threat levels remain low throughout all national and sectoral risk assessments. Namibia's[3] greatest challenge in TF mitigation is ineffectiveness which stems from poor TF controls within supervised institutions, limited TF definition in the PACOTPAA which hampers combatting efforts and inadequate combatting capacity of law enforcement authorities. For these reasons, the overall TF risk rating, at a national level, initially found low in the 2020 NRA has been escalated to Medium with the 2023 NRA update.

It is well established that ML control vulnerabilities can be equally exploited to advance TF activities. For this reason, controls that may be traditionally viewed as necessary for preventing ML are equally essential for preventing and combatting TF activities.

[3] As per Namibia's Mutual Evaluation Report, issued September 2022.

6. UNDERSTANDING THE RISK BASED APPROACH

The RBA speaks to the implementation of a control system premised on a Lending Institution's understanding of risks it may be exposed to. As shown in the diagram below, such understanding is what informs the design, nature and extent of controls implemented to mitigate risks (mitigation plan). The key RBA features are identifying risks, assessing such risks to understand their levels and impact, followed by a mitigation plan aligned to such risk levels. An effective control implementation is also characterised by documenting ML/TF/PF risk findings (in a risk report) and updating such when the need arises. This enables a platform through which risks are tracked.



Risk Based Approach implementation framework

The primary RBA steps can be explained as follows:

a. *Identifying ML/TF risks facing a Lending Institution:* this should be done with consideration of its customers, services, countries of operation, also having regard to publicly available information regarding ML/TF risks and typologies. This process also ensure risks are duly *assessed*, *categorised/classified* or rated to enhance *understanding* of such. The understanding of risks lays the foundation for implementing risk management measures;
b. *Risk management and mitigation:* identifying and applying measures to effectively and efficiently mitigate and manage ML/TF risks;

c. *Ongoing monitoring:* putting in place policies, procedures and information systems to monitor changes to ML/TF risks; and

d. *Documentation:* documenting risk assessments, strategies, policies and procedures to monitor, manage and mitigate ML/TF risks.

The above suggests that access to accurate, timely and objective information on ML/TF risks is a prerequisite for an effective RBA. If duly implemented, the RBA ensures prudent balancing of compliance costs to the Lending Institution and clients by prioritising and directing controls to where they are most needed, in a prudent manner. This ensures high risk clients and services are accorded controls which are commensurate to such risk levels while lower risk clients and services are not burdened with undue customer due diligence.

7. FOUNDATION OF THE RBA: CONDUCTING RISK ASSESSMENTS

The object of understanding client and transaction risks is to help the Lending Institution determine the level of due diligence such client should be subjected to. As mentioned above, access to accurate, timely and objective information on ML/TF risks is a prerequisite for an effective risk assessment and overall RBA. Lending Institutions, like all other Accountable Institutions are best placed to understand their risk exposure and thus implement controls to manage same. This section avails basic guidance around carrying out a risk assessment as a foundation for the RBA, with a focus on indicators of high risk.

7.1 Undertaking ML/TF/PF Risk Assessments[4]

The 2020 NRA rated the sector's ML vulnerability as Medium. Unlike sectors rated Very Low to Low, this rating places the sector amongst the sectors with a greater need to

[4] FIA section 39(1) [Read with FIA section 23]: An accountable institution, on a regular basis, must conduct ML/TF/PF activities risk assessments taking into account the scope and nature of its clients, products and services, as well as the geographical area from where its clients and business dealings originate. Persons much measure, rank or rate (e.g low, medium and high) their level of risk for relevant elements of the services they aim to provide. You should rank each service as low, medium or high risk. The control measures should describe how the entity will reduce each level of risk, especially the medium and higher risk rated levels. The FIC may, in its interpretation however disagree with ratings not duly informed and request reconsiderations accordingly.

ensure effective risk mitigation. The threats are generally low. The vulnerabilities of sectoral control shortcomings largely escalated to such risk rating. With the banking sector, Trade Finance was rated Medium while Micro Credit Products were rated Low, Credit Products for Retail Clients rated Medium Low, Credit Products for SMEs were rated Medium Low while Credit Products for Large Businesses were rated Low.

A Lending Institution's risk assessment comprehensiveness should be aligned to the nature, complexity and risk exposure of its products and services (or amendments to such). ML/TF risks can be organised into three categories: (a) client risks; (b) risks associated with services rendered (and associated delivery channels); and (c) country or geographic risks. The risks and red flags listed in each category herein below are not exhaustive but provide a starting point for Lending Institutions to consider when assessing risks or designing their RBA. The weight given to these risk categories (individually or in combination) in assessing the overall risk of potential ML/TF may vary given the size, sophistication, nature and scope of services provided. These criteria, however, should be considered holistically and not in isolation. Lending Institutions, based on their individual practices and reasonable judgements, will need to independently assess the weight to be given to each risk factor.

Below is guidance on such categories of risks:

7.1.1 Evaluating Client Risk Profiles

The key risk factors that increase a client's ML/TF/PF risk profile to Lending Institutions include:

a. ***Inherent risk levels of different types of legal persons and arrangements:*** *The ability for criminals to hide their identity behind complex legal structures when conducting commercial transactions remains an attractive characteristic of legal persons and such other arrangements for ML/TF purposes. Below are results from the 2023 NRA update showing ML threats of various legal persons and trusts.*

CASES REFERRED FOR FURTHER INVESTIGATIONS: PERIOD: 2009 - 2021				
	Total STRs Received	***No. of Cases (SDs)***	***Total Financial Value from such Cases/SDs (NAD)***	***Average Financial value Per Case (NAD)***
Close Corporations (CCs)	*228*	*104*	*34,807,766,160.75*	*334,690,059*
Companies	*232*	*115*	*8,659,067,618.13*	*75,296,240*
Trusts	*96*	*55*	*1,613,992,815.33*	*29,345,323*
Natural Persons	*5,690*	*1,696*	*23,404,719,080.81*	*13,799,952*

Vulnerabilities with Close Corporations (CCs): *The 2023 NRA update suggests that CCs are **the most abused type of legal persons** in terms of financial values[5]. This observation suggests that large scale ML in terms of financial values or impact is more likely to be advanced through CCs and to a lesser extent through companies and trusts.*

CASES REFERED FOR INVESTIGATIONS, PER PREDICATE OFFENCE: PERIOD: 2009 – 2021						
	Fraud	***Total Financial Value (NAD)***	***Potential Tax Evasion***	***Total Financial Value (NAD)***	***Corruption***	***Total Financial Value (NAD)***
Close Corporations (CCs)	*25*	*404,533,140*	*66*	*28,400,797,080*	*7*	*394,575,890*
Companies	*56*	*656,836,151*	*141*	*738,080,077*	*35*	*284,419,187*
Trusts	*3*	*14,016,585*	*7*	*776,270,899*	*6*	*56,516,585*
Natural Persons	*667*	*1,695,855,636*	*2264*	*15,632,296,444*	*84*	*1,955,490,671*

[5] As per cases analysed by the FIC and referred to various investigative authorities on findings that suggest possible ML.

The high number of natural persons possibly implicated in ML activities still suggests that, by and large, people advance ML activities in their individual capacities, if the 2023 NRA update findings are anything to go by. Some STRs/SARs within the FIC suggests higher risks arise when there is a suspected use of personal funds for business purposes, or vice-versa.

Vulnerabilities with trusts: *In Namibian, a trust can either be a private trust or a public charitable trust. The 2023 NRA update suggests only inter-vivo trusts[6] may have been abused in advancing ML will all of them being (100%) Namibian initiated or founded (owned). None such trusts in ML or related predicate offence investigations are charitable trusts. The NRA further found that about 82% of these trusts have Namibian donors and Namibian trustees. Only 40% of the trusts involved in potential ML cases have foreign nationals listed as beneficiaries, with the majority being South African citizens.*

b. Complex ownership or legal structures: *Should be viewed along with observations above. Where the entity structure or nature of the entity or relationship makes it difficult to easily identify the true beneficial owners, directorships or controlling interests or clients attempting to obscure understanding of their business, ownership or the nature of their transactions, such as:*

i. ***Uncommon ownership structures****, especially when spread across different countries, which makes it difficult to trace the natural persons (without reasonable business grounds) who ultimately own, direct or manage entities;*

ii. *Unreasonable use of* ***shell and/or shelf companies, front companies****, legal entities with ownership through nominee shares or bearer shares, control through nominee or corporate directors, legal persons or legal arrangements splitting company incorporation and asset administration*

[6] Trusts created between living persons registered under the Trust Moneys Protection Act 34 of 1934.

over different countries, all without any apparent legal or legitimate tax, business, economic or other reason;

iii. ***Unexplained use of informal arrangements*** *such as family or close associates acting as nominee shareholders or directors without any apparent legal or legitimate tax, business, economic or other reason; and*

iv. *Use of* ***trust structures for tax evasion or to obscure ownership*** *in order to place assets out of reach to avoid future liabilities.*

c. *High risk of non-face-to-face clients or beneficial owners:* *Should be viewed along with observations above. Non-face-to-face clients or beneficial owners on whose behalf transactions are undertaken present inherently higher ML/TF/PF risks;*

d. *Use of Nominees:* *Namibia's Mutual Evaluation*[7] *found that "… legal persons are allowed to have nominee shareholders and directors in terms of the companies act. However, there is no mechanism to prevent the misuse of legal persons by requiring the nominee shareholder and directors to disclose their identities, to be licensed for their nominee status to be included in company registries or any other mechanism identified by Namibia." The use of nominees increases ML/TF/PF risks. Below is a non-exhaustive list of indicators suggesting undisclosed nominee arrangements:*

i. *the profile of a trustee, director or shareholder is inconsistent with the activities of the trust, company or other legal entity;*

ii. *the individual holds a number of appointments to unconnected trusts, companies or other legal entities;*

iii. *a nominee's source of wealth is inconsistent with the value and nature of the assets within the trust, company or other legal entities;*

iv. *funds into and out of the trust, company or other legal entity are sent to or received from unidentified third party/ies;*

[7] See Page 171, Under Recommendation 24, Criterion 24.12.

v. *a Legal Practitioner is accustomed to acting on the instructions of another person who is not the trustee or director or other natural person exercising effective control; and*

vi. *Requests or instructions are subject to little or no scrutiny and/or responded to extremely quickly without challenge by the individual/s purporting to act as the trustee, director/s or other natural person exercising effective control.*

e. ***Known convicts or persons charged with proceed generating crimes:*** *Clients with previous convictions for crimes that generate proceeds, including clients associated with adverse/negative media reports as being linked to financial crimes are naturally high-risk;*

f. ***Politically Exposed Persons (PEPs)[8]:*** *This includes both domestic and international (PEPs). All PEPs are inherently high risk for ML/TF/PF. Comparatively, foreign PEPs present a higher risk than domestic PEPs, naturally as their CDD information cannot[9] be effectively or readily verified with relevant domestic authorities. PEPs need to be subjected to Enhanced Due Diligence (EDD) which include obtaining management approval before facilitating deals involving them, as per FIC Guidance Note 01 of 2019;*

g. ***High net worth individuals:*** *They usual deal in comparatively higher amounts than the average customer. It is challenging to determine how much funds are within or outside their expected financial profile. One can thus not easily tell when they transact beyond their means, co-mingling licit with illicit funds etc. Depending on other factors such as they type of industries, Lending Institutions need to be reasonably cautious and if need be, conduct EDD with high networth clients;*

[8] Note that the proposed FIA amendments rather speak of a Prominent Influential Person (PIP). Similar to a PEP. See FIC Directive No. 02 of 2020 on PEPs as well as Guidance Note No. 01 of 2019 on the definition and due diligence required for PEPs: Both documents are available on the FIC Website under the "Publications" folder.

[9] Risk assessments should thus always consider the reliability of national identification systems in foreign countries and the effectiveness of AML/CFT/CPF controls countries where clients originate from or have ties with.

h. ***Exposure to Cryptocurrencies (Virtual Assets):*** *Cryptocurrencies are mostly poorly regulated and thus present higher ML/TF/PF risks. Their nature of operations encourage anonymity, which increases risk exposure. It is commonly accepted that launderers would naturally target cryptocurrency platforms as a means to launder proceeds because of poor control frameworks and enhanced anonymity in such sphere;*

i. ***Inexplicable or unreasonable ownership changes:*** *changes in entity directorship and ownership increases risk exposure to the Lending Institution. Equally, the following indications increase risks:*

- *when the legal structure has been altered frequently and/or without adequate explanation (e.g. name changes, transfer of ownership, change of beneficiaries, change of trustee or protector, change of partners, change of directors or officers);*
- *Frequent or unexplained change of professional adviser(s) or members of management of the trustee, company or other legal entity; and*
- *The transfer of the seat of a company to another jurisdiction without any genuine economic activity in the country of destination poses a risk of creation of shell companies which might be used to obscure beneficial ownership.*

Tip – Practical Risk Identification
In practice, the overall risk is assessed periodically and client profile types/pools are identified, which can for example be: Foreign PEP, Domestic PEP, Self-Employed businessman, Foreign Investor, Domestic Investor, Government Employee, Teacher, Bank Manager/Employee etc. Inherent risk levels (high, medium, low) are then assigned to each such profile/type/pool. When a client's loan is approved or is onboarded, he or she is placed in one of such profiles and then subjected to due diligence relevant for such profile. Such due diligence must then include reviewing information which may be specific to such individual client.

7.1.2 Evaluating transaction/service and associated delivery channel risk

Below is a non-exhaustive list of factors which increase the risk of transactions/services and associated delivery channels of such:

a. ***Earlier redemption of loans:*** *This speaks to when loans are settled earlier than initially agreed with a lending institution, usually through one or a few lump sum payments. It may not always be suspicious as additional funds could be realised from other legitimate sources. Lending Institutions should however do the necessary due diligence to establish source of additional funds when client settles loans in earlier than agreed timelines;*

b. ***Additional funds in periodic payments:*** *when additional funds are paid along with the periodic repayment commitments, there is a risk that such additional funds could be sourced from illicit activities and introduced or layered in the formal financial system through loan repayments. The point of departure is first detecting when a client is making additional payments and then conducting due diligence where such appear beyond the client's financial profile;*

c. ***No concerns around higher interest rates/repayments:*** *a transaction which appears uneconomic or inefficient is higher risk for ML and TF. Criminals do not mind slight losses at the opportunity of 'washing' their significant proceeds;*

d. ***Cash:*** *Customers making cash payments are inherently presenting higher ML/TF/PF risks. Also, clients from cash intensive sectors inherently present higher ML risks. Cash has limited audit trail, if any, making it an easier way to move around proceeds of crime without leaving traceable trails of such movements;*

e. ***Use of multiple accounts:*** *When client uses multiple accounts, especially at several financial institutions for no apparent reason, it can be suspicious as they may be trying to structure huge amounts with different institutions. In some cases,* *Lending Institutions need to be wary of clients using one or more foreign bank accounts for no apparent reason as such increases both ML and TF risks;*

f. ***Unexpected resuscitation:*** *Sudden activity from a previously dormant entity or client without a clear explanation.*

7.1.3 Considering Country or Geographic risk

If a client is associated with a high risk jurisdiction, they inherently increase risk exposure to the Lending Institution. There is no universal standard of what a high risk jurisdiction within the AML/CFT/CPF framework is. Best practices, noted from the FATF[10], amongst others, largely guide considerations in this regard. Factors that are generally agreed to place a country in a higher risk category include, but are not limited to the following:

a. ***Foreign customers:*** *Generally, and all things being equal, foreign clients are inherently higher risk than resident/Namibian clients because their identification and such related information cannot be readily identified. If a loan is extended to a legal person or trust, the directors or those exercising effective control of same needs to be identified and subjected to the necessary due diligence. With foreign clients, some could hail from countries with inadequate identification frameworks. There is also a possibility that such clients could be linked to complex and opaque legal structures internationally, a factor which may further increase their inherent risk profile;*

b. ***Prevalence of crime, instability, terrorism, proliferation etc:*** *Other than poor national identification frameworks as per above, in some countries, client risk can also be increased if a country a client is associated with has higher levels of bribery and corruption, tax evasion, capital flight, conflict zones, war, terrorism and organised crime within or within neighbouring[11] states. Information about high-risk jurisdictions is widely available, which is detailed from several open-source documents and media.*

---

[10] Guidance for a Risk Based Approach: TCSPs, accessed via file:///C:/Users/ham638/Downloads/RBA-Trust-Company-Service-Providers%20(4).pdf

[11] it could also be neighbouring countries as money laundering or terrorist financing often involves the movement of funds across borders.

The following are indications, based on credible sources, which may escalate the risk of a country that clients to a transaction may be associated with. These are countries:

- *that have been found by organisations such as FATF, World Bank, Organisation for Economic Cooperation and Development (OECD) and the International Monetary Fund (IMF) as not having ineffective AML/CFT/CPF measures in place;*
- *identified to be uncooperative in extraditions and providing beneficial ownership information to competent authorities, a determination of which may be established from reviewing FATF Mutual Evaluation reports or reports by organisations that also consider various co-operation levels such as the OECD Global Forum reports on compliance with international tax transparency standards;*
- *areas identified by credible sources as providing funding or support for terrorist activities or that have identified/designated (e.g by other countries) terrorist organisations operating within them;*
- *identified as being a major source or a major transit country for illegal drugs, human trafficking and smuggling and illegal gambling;*
- *not subject to equivalent AML/CFT/CPF measures; and*
- *subject to sanctions or embargoes issued by international community including the UN, OFAC, EU etc.*

In addition to the above, client risk is increased if information at hand or from other sources links clients to being involved in dealings with the following: oil, arms and weapons, precious metals and stones, tobacco products, cultural artefacts; and ivory and other items related to protected species. The Lending Institution's periodic risk assessment should indicate the inherent risk level of different countries (or come up with risk levels for countries that meet certain criteria). This aids risk considerations for each foreign client.

7.2 Role of Key Partners/Stakeholders

The provision of some services in the sector may require inputs or responsibilities undertaken by partners or stakeholders of the Lending Institution (or a bank along the value chain/in the deal/transaction). If such partnership/arrangement exists, the Lending Institution should duly understand the nature and effectiveness of AML/CFT/CPF controls that are implemented by such partners or stakeholders in the value chain, should one choose to rely on such. Ensure that such partners or stakeholders have capacity and are willing to play their part in ensuring effective risk mitigation as per the FIA, as the law does not at present permit reliance on controls enacted by another Accountable Institution (apart from record keeping).

7.3 Type, Nature and Extent of Controls

To reduce inherent[12] risks to tolerable or acceptable residual[13] levels Lending Institutions have a responsibility to implement controls and duly demonstrate their effectiveness to authorities such as the FIC. The FIC, as supervisory body must be satisfied, upon such presentation, that such residual risk levels are tolerable or acceptable to the national AML/CFT/CPF framework. The entirety of controls, aligned to risks, should be documented in an AML/CFT/CPF Program or Policy document which needs management approval.

7.4 External Risk Assessments

The considerations and indicators herein are not exhaustive. Lending Institutions are required to consider observations from SRAs and NRAs issued by the FIC. Local[14] and international trends and typology reports issued by bodies such as ESAAMLG[15] and FATF[16] (available on their websites) equally help highlight changing risks broadly and

---

[12] Inherent risks refer to the level of (original) risks prior to the implementation of controls to reduce the likelihood and impact of such risks.
[13] The remaining risk level after due controls have been implemented.
[14] Published on the FIC website under Risk Assessments folder while trends and typology reports are under Publications folder.
[15] https://www.esaamlg.org/index.php/methods_trends
[16] https://www.fatf-gafi.org/en/publications.html

related to the sector. To the extent possible, this guidance has incorporated lessons and best practices from such local and international publications. ML and TF trends are dynamic, it is thus essential to keep abreast of updated publications in this regard.

8. FURTHER GUIDANCE ON CONTROLS

This Guidance Note deals with risk assessments as a foundational step for the implementation of an effective Risk Based Framework within Lending Institutions. Lending Institutions are further required to duly study Guidance Note 17 of 2023 which speaks to the practical implementation of controls to mitigate ML/TF/PF risks at institutional level. The FIC website contains several other Directives, Guidance Notes, Circulars and Regulations which avail helpful guidance on measures to combat ML/TF/PF in terms of the FIA.

9. GENERAL

This document may contain statements of policy which reflect the FIC's administration of the legislation in carrying out its statutory functions. This guidance is issued without prejudice to the FIA and its complementing Regulations. The information contained in this document is intended to only provide a summary on these matters and is not intended to be comprehensive.

10. NON-COMPLIANCE WITH THIS GUIDANCE

This document is a guide. Effective implementation is the sole responsibility of Lending Institutions. Should an institution fail to adhere to the guidance provided herein, it will be such institution's responsibility to demonstrate alternative risk management controls implemented which are effective to the FIC's satisfaction as the supervisory authority.

The Guidance Note can be accessed at www.fic.na

DATE ISSUED: 06 JULY 2023

DIRECTOR: FINANCIAL INTELLIGENCE CENTRE

FIC CONTACT DETAILS

All correspondence and enquiries must be directed to:
The Director, Financial Intelligence Centre
P.O. Box 2882
No. 71 Robert Mugabe Avenue, Windhoek
helpdesk@fic.na