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. 14 OF 2023

GUIDANCE ON RISK ASSESSMENTS AND ML/TF/PF INDICATORS

LEGAL PRACTITIONERS AND LAW FIRMS

First Issued: 05 July 2023

TABLE OF CONTENTS

1. BACKGROUND 7
2. COMMENCEMENT 7
3. SCOPE OF SERVICES DESIGNATED IN THE FIA 8
3.1 Item 1 of Schedule 1 of the FIA 8
3.2 Item 3 of Schedule 1 of the FIA 8
4. GENERAL VULNERABILITIES OF LEGAL PRACTITIONERS 9
4.1 Abusing Corporate Vehicles 9
4.2 Abusing Real Estate for ML/TF Purposes 9
5. BALANCING ACT 10
6. ML RISKS IN LEGAL PRACTITIONERS 11
7. TF RISKS IN LEGAL PRACTITIONERS 12
7.1 Helpfulness of ML Controls for TF 13
7.2 Transnational Risks of TF 13
7.3 Nature/Sources of TF funds 13
7.4 Size of Funds for TF 14
7.5 Covert Nature of TF Suspicions 15
7.6 Study Publications on TF Indicators, Trends and Typologies 15
7.7 TF Risks Associated With NPOs 16
7.8 Exposure to Cryptocurrencies (Virtual Assets) 16
7.9 Screening Against Sanctions Lists 17
7.10 Potential Origin of TF Threats 17
7.11 Namibia as a Conduit for TF 18
8. UNDERSTANDING THE RISK BASED APPROACH 18
9. FOUNDATION OF THE RBA: CONDUCTING RISK ASSESSMENTS 20
9.1 Practical Risk Assessment and Documenting Outcomes 20

9.2 Undertaking ML/TF/PF Risk Assessments 21
9.3 Role of Key Partners/Stakeholders..... 39
9.4 Type, Nature and Extent of Controls 40
9.5 External Risk Assessments 40
10. FURTHER GUIDANCE ON CONTROLS..... 40
11. GENERAL..... 41
12. NON-COMPLIANCE WITH THIS GUIDANCE..... 41

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;

"LEAs" means Law Enforcement Authorities such as the Namibian Police, Anti-Corruption Commission or NAMRA;

"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;

"Single Transaction" means a transaction other than a transaction concluded in the course of a business relationship;

"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;

“TCSPs” within the context of this Guidance, refers to all types of Accountable Institutions providing Trust and Company Secretarial Services as per Items 1 (c – f) and 3 of Schedule 1 of the FIA. These are services related to company secretarial activities including, but not limited to the formation of legal persons and arrangements including trusts. Some Accountants, Legal Practitioners and Financial Institutions also provide these services.

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. It contains Guidance that should be considered along with Guidance Note 15 of 2023 which explains how Legal Practitioners[1] should implement controls which are risk based or informed by risks.

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 Legal Practitioners listed in Schedule 1, Items 1 and 3 of the FIA. These are essentially Legal Practitioners involved in the buying and selling of real estate; the creation of companies, trusts, partnerships etc., as well as managing funds and assets on behalf of clients. This guidance note applies to all such Legal Practitioners practising or availing such services as part of a firm or in any other capacity as part of their business. In this context, they are all collectively referred to as Legal Practitioners.

It is common cause that services offered by Legal Practitioners have been abused for ML domestically. Internationally, there are trends and typologies which suggest such abuse to advance TF/PF activities. To help mitigate ML/TF/PF risks, the Financial Intelligence Centre (FIC) issues this Guidance to help Legal Practitioners 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 **06 July 2023**.

[1] a legal practitioner as defined in the Legal Practitioners Act, 1995 (Act No.15 of 1995).

3. SCOPE OF SERVICES DESIGNATED IN THE FIA

Not all services offered by Legal Practitioners are designated in the FIA. The FIA, as per international standards takes a Risk Based Approach (RBA), which advocates for only covering services deemed highly exposed to ML, TF and PF risks.

3.1 Item 1 of Schedule 1 of the FIA: Legal Practitioners when they render the following services:

(a) "Buying and selling of real estate for cash or otherwise;

(b) Managing of client money, securities, bank or securities accounts or other assets;

(c) Facilitating or sourcing contributions for the creation, operation or management of legal persons or arrangements;

(d) Creation, operation or management of legal persons or legal and commercial arrangements;

(e) Buying and selling of business entities, or parts thereof; and

(f) Buying and selling of legal rights."

3.2 Item 3 of Schedule 1 of the FIA: A Legal Practitioner when they avail typical Trust and Company Secretarial Services (TCSS) as per Item 3 of Schedule 1 of the FIA. This is when they prepare for and carry out transactions for their client in relation to the following activities -

(a) "acting as a formation agent of legal persons;

(b) acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;

(c) providing a registered office; business address or office accommodation, correspondence or administrative address for a company, a partnership or any other legal person or legal or commercial arrangement;

(d) acting as (or arranging for another person to act as) a trustee of a trust; and

(e) acting as (or arranging for another person to act as) a nominee shareholder for another person."

4. GENERAL VULNERABILITIES OF LEGAL PRACTITIONERS

4.1 Abusing Corporate Vehicles

Companies, trusts and other similar legal arrangements are seen by criminals as potentially useful instruments through which to hide their criminal proceeds or commit illicit activities, amongst others.

Shell companies, which do not have any ongoing business activities or assets, may be used for legitimate purposes such as serving as a transaction vehicle. They may also be used to **conceal beneficial ownership, or enhance the perception of legitimacy by criminals**. Criminals may also seek to misuse shelf companies formed by Legal Practitioners by seeking **access to companies that have been 'sitting on the shelf' for a long time**. This may be in an attempt to **create the impression that the company is reputable and trading in the ordinary course because it has been in existence for many years**. Shelf companies can also add to the overall complexity of entity structures, further concealing the underlying beneficial ownership information.

In some instances, criminals may want to acquire shares or ownership in entities to legitimise their operations. Similarly, they may want to use trusts and such legal arrangements to hide their ill-gotten proceeds. Legal Practitioners and Trust and Company Service Providers are gatekeepers to the financial system as they are in a position to facilitate such acquisitions and access to trusts, amongst others.

4.2 Abusing Real Estate for ML/TF Purposes

Criminals seek the opportunity to retain control over criminally derived assets while **frustrating the ability of law enforcement to trace the origin and ownership of the assets.**

Money laundering through real estate transactions **integrates ill-gotten funds into the financial system (legal economy) while providing a safe investment**. It allows criminals to enjoy assets and derived funds having camouflaged the origin of the money used for payment. A number of techniques are used, namely cash or opaque financing schemes, overvalued or undervalued prices, and non-transparent companies and trusts or third parties that act as legal owners. Among the possible indicators are clients purchasing assets beyond their known financial profile, geographical features (such as the distance between the property and the buyer and their actual geographical centre of interest) etc. In order to assess the existence of a money-laundering risk, concrete assessments of transactions and a customer's profile, transactions/conduct or situation provide indications that help raise red flags and trigger reporting obligations.

5. BALANCING ACT

The greater social and economic impacts that befalls a society were reckless or unhindered criminality prevails are reasons for the international community's stance on combatting ML, TF and PF risks. With Namibia being a Member State of the United Nations, the FIA is aligned to such.

Combatting ML, TF and PF risks, like all other financial crimes that the Legal Profession is exposed to, requires striking the right balance between risk management on the one hand and applying the required degree of legal professional privilege. The latter comes with consequences which may impair constitutionally guaranteed rights, if not duly administered. In the same vein, legal professional privilege or professional secrecy does not protect a Legal Practitioners from knowingly facilitating a client's illegal conduct. The FIA accords Legal Practitioners instruments to place themselves in a position to mitigate risks of abuse by criminals. Creating an environment which harmonizes the practical risk management with respect for human rights is what the FIA advocates for with its cautious approach to the RBA. It is therefore very important that risk assessments are effective to help Legal Practitioners identify clients and transactions which needs to be duly subjected to due diligence.

6. ML RISKS IN LEGAL PRACTITIONERS

It may be difficult to distinguish a money launderer trying to use complex legal structures, legal persons or trusts to hide or move their illicit funds from a legitimate beneficial owner who simply wants a legal entity to use for one or other reason. Generally, the money laundering process can be described as follows:

A. Placement

Involves placing the proceeds of crime in the financial system. *For example, buying a legitimate business with proceeds of crime or with the intention of using the books/accounts of such legitimate business to move proceeds of crime or introduce such in the financial system.*

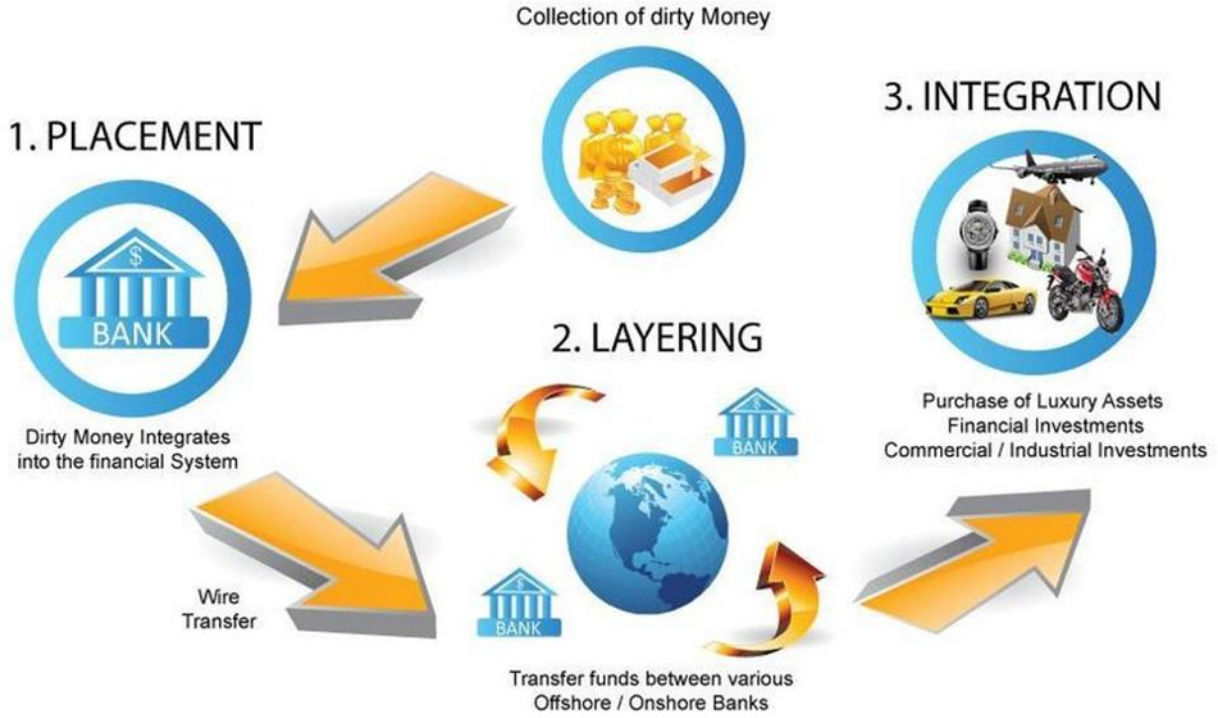
B. Layering

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 is presented or used as if such are from legitimate origins. In some instances, assets bought with proceeds of crime are leased in legitimate commercial transactions to generate what would be 'legitimate funds'.*

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.

Below is a diagram of the three layers of ML.



Legal Practitioners, as part of their risk assessment process, should assess the ML/TF/PF vulnerabilities and high-risk factors associated with each of their clients accessing the services they offer. The risk assessment section herein avails indicators of potential high risks. Such should be duly considered for combatting ML, TF and PF.

7. TF RISKS IN LEGAL PRACTITIONERS

While the 2012 National Risk Assessment (NRA), 2017/18 update and 2020 NRA rightly suggest that ML risks are more frequent and prominent. TF risk levels rated low in the 2020 NRA are escalated to Medium with the 2023 NRA update. It is well established that ML control vulnerabilities can be equally explored 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. This section speaks to TF risk considerations generally and specifically for Legal Practitioners.

7.1 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. Namibia has not observed potential TF exposure within the Legal Practitioners sector. This does not however mean the sector is not vulnerable to such abuse. The creation of legal persons and trusts for example, 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] vulnerable to TF abuse.

7.2 Transnational[3] Risks of TF

The 2020 NRA and 2023 NRA update observe that whilst Namibia is not considered high-risk for TF, even small-scale financing raised from within Namibia could have a significant impact if combatting measures fail. When looking at the risk of non-Namibian clients, Legal Practitioners should consider not only high-risk countries but also their neighbouring countries, as TF often involves the movement of funds or assets across borders. The 2020 NRA in particular, equally found that Namibia's porous borders present a significant vulnerability which enhances the ease with which proceeds can be moved in and out of the country. Generally, control vulnerabilities exploited by TF threats can be similarly exploited by PF threats. This context is helpful to bear in mind in this section as Legal Practitioners equally have an obligation to combat PF.

7.3 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

[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.
[3] Extending or operating across national boundaries

relies on similar methods (control vulnerabilities) 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. 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.

Importantly, the risks associated with TF are highly dynamic. As such, Legal Practitioners need to ensure that their prevention and combatting measures are current, regularly reviewed and flexible. 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.

7.4 Size of Funds for TF

Transactions associated with TF may be conducted in very small amounts, which in applying a risk-based approach could be the very transactions that are frequently considered to be of minimal risk with regard to ML. This is a bigger challenge for Legal Practitioners that do not naturally deal in financial services but legal services. Where funds are from legal sources, it is even more difficult to determine if they could be used for terrorist purposes. The need to be mindful of ML indicators for TF is valuable but a Legal Practitioner's AM/CFT policy/procedures have to deliberately distinguish controls aimed at detecting potential TF.

7.5 Covert Nature of TF Suspicions

In addition, the actions of those supporting terrorist activities may be overt (openly) and outwardly innocent in appearance, such as the purchase of shell, or shelf companies or take-over of existing businesses to further their goals, with the only covert (hidden) fact being the intended criminal use of such legal persons. Therefore, while terrorist funds may be derived from criminal activity as well as from legitimately sourced funds, transactions related to TF may not exhibit the same traits as conventional ML, and thus challenging to detect.

TF covers a wide range of terrorism-related activity, including operational funds, equipment, salaries and family compensation, social services, propaganda (e.g radicalization), training, travel, recruitment and corruption. However, in all cases, **it is not the responsibility of the Legal Practitioners to determine the type of underlying criminal activity or intended terrorist purpose as a pre-requisite for reporting TF (or ML) suspicions**. The Legal Practitioner's role is to simply identify, report the suspicion *without delay*, *freeze any funds or assets* of such subject, *prohibiting* further transacting of such subjects while treating same with the *necessary sensitivity*. The FIC and relevant Law Enforcement Authorities have the responsibility to examine the matter further and determine/confirm if there is a link to TF.

7.6 Study Publications on TF Indicators, Trends and Typologies

TF detection efforts, absent of specific national/international guidance and typologies may be limited and inadequate. Such is likely to be based on monitoring that only focuses on transactions with countries or geographic areas where terrorists are known to operate or on the other limited typologies available[4]. The ability of Legal Practitioners to detect and identify potential TF red flags or suspicions can be enhanced with guidance on TF (and

[4] Many of which are indicative of the same techniques as are used for ML.

ML) typologies, risk assessment outcomes or acting on specific intelligence provided by authorities. The sector is therefore encouraged to duly consider the high risk indicators in section 9.2 herein, along with FIC publications such as the SRAs, NRAs and relevant TF related reports on the FIC website[5] and other sources[6].

7.7 TF Risks Associated With NPOs

It is internationally accepted that some NPO-types or their services can be easily abused to advance terrorism activities. This typically happens with NPOs abusing the legitimacy and social trust that the sector enjoys for resourcing or financing terrorist activities directly or indirectly. In Namibia[7], religious or Faith Based Organizations (FBOs) were identified as the high-risk sub-sector within NPOs. The 2023 NRA update found NPOs involved in charitable services/activities to be equally highly exposed to TF risks.

Legal Practitioners need to apply the necessary level of due diligence when availing their services for the creation of religious/FBOs and charitable NPOs or any dealings involving such NPOs. It is a given that some NPOs register section 21 companies through Legal Practitioners. Due Diligence, as per Guidance Note 15 of 2023 is required with such registrations. Amongst other controls, Legal Practitioners have to ensure due identification of those managing or directing the affairs of such NPOs and obtain information to gain assurance that proceeds or values related to such NPO/deals are not linked with persons associated with terrorism activities. It is also helpful to gain assurance that such NPOs are not subject to adverse reports around their governance frameworks, nor have associations with high-risk countries or terrorist groups.

7.8 Exposure to Cryptocurrencies (Virtual Assets)

[5] https://www.fic.na/ see under ML/TF/PF Risk Assessments - https://www.fic.na/index.php?page=mltfpf-risk-assessment-reports; Trends and Typologies -https://www.fic.na/index.php?page=trends-and-typologies and amongst others.
[6] Guidance for a Risk Based Approach: TCSPs, accessed via file:///C:/Users/ham638/Downloads/RBA-Trust-Company-Service-Providers%20(4).pdf
[7] 2020 NRA.

Cryptocurrencies, because of their very nature, are mostly poorly regulated and thus present higher TF and ML risks. Risks are increased when clients of Legal Practitioners are involved in cryptocurrencies in one way or the other. Cryptocurrencies can easily facilitate the transfer of value to higher risk jurisdictions.

7.9 Screening Against Sanctions Lists

As explained in Directive 01 of 2023, Guidance Notes 07 and 15 of 2023 as well as several other FIC publications, Legal Practitioners need to continue screening of all parties involved in services they provide in addition to the measures mentioned herein.

7.10 Potential Origin of TF Threats

As per the various domestic SRAs, NRAs and consideration of TF trends internationally, the FIC highlights the following as primary TF threats Accountable Institutions, including Legal Practitioners, should consider:

a. *Overseas groups able to inspire support through radical ideology* – Individuals may be inspired to contribute to overseas terrorist groups by travelling to conflict zones, which requires self or third-party funding. Radicalised individuals may also choose to contribute to terrorism by raising and contributing funds;

b. *Well-resourced groups with established networks* – This may involve the movement of larger sums of money for terrorism, in particular for or by state-sponsored groups; and

c. *Domestic terrorism* – given the low-to-non-existent level of domestic support for terrorist causes and absence of terrorist networks, it is more likely that financiers of domestic terrorism (if it were to happen domestically) could manifest in Namibia as isolated disaffected individuals or small groups.

Legal Practitioners need to duly identify their clients, assess their risk profiles to minimize abuse from those who may be radicalized or somehow use legal persons and arrangements to somehow move or raise funds to advance TF.

7.11 Namibia as a Conduit for TF

The enhanced TF risk associated with foreign clients, especially those from high-risk countries, who are involved in property deals, creating or changing beneficial ownership status with legal persons and trusts, cannot be overemphasized. One of the potential consequences of transnational ML is that channels may be established that may also be exploited by terrorist financiers. Overseas groups may seek to exploit Namibia as a source or conduit for funds to capitalise on Namibia's reputation as being a lower risk jurisdiction for TF. For instance, funds originating in or passing through Namibia may be less likely to attract suspicion internationally.

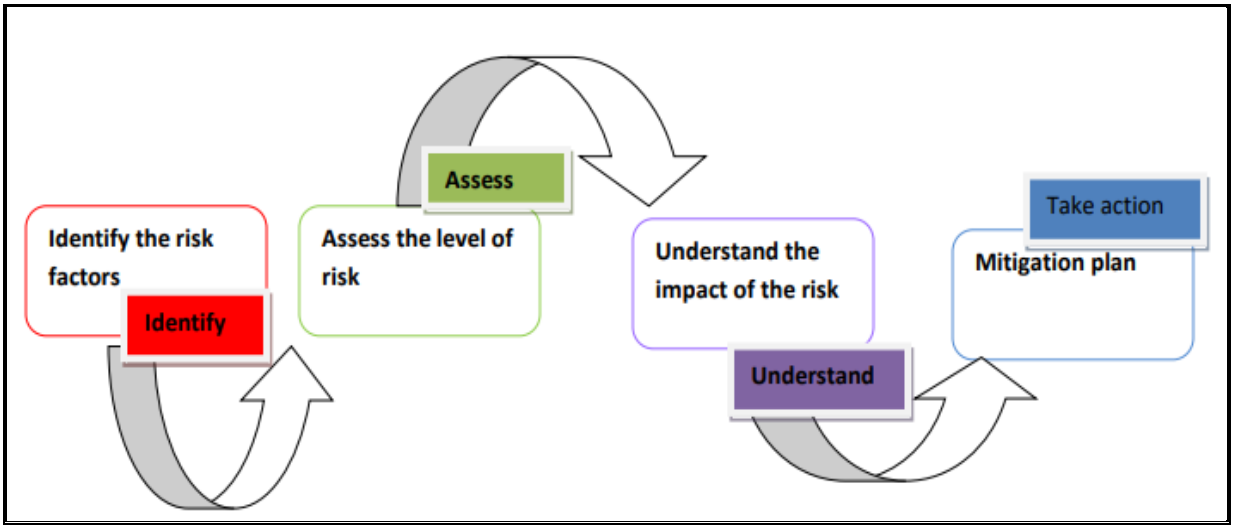
The same methods explained above through which Legal Practitioners can be abused to advance TF are similar for PF. The due diligence and RBA, especially screening of clients/parties to transactions against sanctions lists is essential in combatting both TF and PF within the sector.

8. UNDERSTANDING THE RISK BASED APPROACH

The basic intent behind the Legal Practitioners' FIA obligations, as derived from international obligations, is to ensure that their services and operations are not abused for facilitating criminal activities and specifically ML/TF.

The RBA speaks to a control system premised on a Legal Practitioner'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 its 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 Legal Practitioner:* 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*, 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 business and customers 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 unwarranted stringent customer due diligence.

9. FOUNDATION OF THE RBA: CONDUCTING RISK ASSESSMENTS

The object of understanding client and transaction risks is to help the Legal Practitioner determine the level of due diligence such client should be subjected to. The principle in AML/CFT/CPF due diligence is that low risk clients making use of low risk services should be subjected to minimum or simplified due diligence. On the other hand, higher risk clients should be subjected to Enhanced Due Diligence (EDD). The nature and extent of EDD is dependent on the level of assurance/comfort that a TCSP needs to gain in reducing its ML/TF/PF risk exposure. 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.

Legal Practitioners, 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.

9.1 Practical Risk Assessment and Documenting Outcomes

a. All identified risks as far as clients and transactions are concerned should be **documented in Risk Management Reports**. Such report(s) (assessment outcomes) should be periodically updated when material changes arise in risks and controls;
b. Each of the risks could be assessed **using indicators such as low risk, medium risk and/or high risk**. A short explanation of the reasons for each attribution should be included and an overall assessment of risk determined. An action plan (if required) should then be outlined to accompany the assessment and dated.

Action plans can help identify potential red flags, facilitate risk assessment and decide on CDD measures to be applied;

c. A risk assessment of this kind should not only be carried out for each specific client and service on an individual basis, as required, but also to **assess and document the risks on a firm-wide basis, and to keep risk assessment up-to-date** through monitoring of the client relationship. The written risk assessment should be made accessible to all professionals having to perform AML/CFT duties. Proper safeguards should be put in place to ensure privacy of clients;

d. The written risk assessment **outcomes should be made accessible to all professionals having to perform AML/CFT duties**. Where legal professionals are involved in longer term transactions, risk assessments should be undertaken at suitable intervals across the life of the transaction, to ensure no significant risk factors have changed in the intervening period (e.g new parties to the transaction, new sources of funds etc.); and

e. A final risk assessment should be **undertaken before a transaction is completed**, allowing time for any required STR to be filed and any authority to move or transfer assets to be obtained from law enforcement.

9.2 Undertaking ML/TF/PF Risk Assessments[8]

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 ensure effective risk mitigation.

[8] 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.

The comprehensiveness of risk assessments should be aligned to the nature, complexity and risk exposure of a Legal Practitioner's products and services (or amendments to such). ML/TF risks can be organised into three categories: (a) client risk ; (b) risks associated with services rendered (and associated delivery channels); and (c) country/geographic risk. The risks and red flags listed in each category herein below are not exhaustive but provide a starting point for Legal Practitioners to use 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 by the Legal Practitioner and/or law firm. These criteria, however, should be considered holistically and not in isolation. Legal Practitioners, 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:

9.2.1 Evaluating Client Risk Profiles

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

a. ***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[9]. 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. There is a significant number of legal persons, especially CCs that are constantly used in the fraudulent transfer of fraudulent cases involving questionable property sales. Based on complaints filed with BIPA, STRs with the FIC and direct reports to the Namibian Police, the lengthy, but often reliable normal property transfer process is fast tracked through the change of CC beneficial ownership when such CC owns property[10].*

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*

[9] As per cases analysed by the FIC and referred to various investigative authorities on findings that suggest possible ML.
[10] Also reflected in the Mutual Evaluation Report of Namibia, paragraph 395. Page 118.

Natural Persons	*667*	*1,695,855,636*	*2264*	*15,632,296,444*	*84*	*1,955,490,671*

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[11] 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 structure: *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 owner 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. Unexplained use of ***shell and/or shelf companies, front companies****, legal entities with ownership through nominee shares or bearer shares,*

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

control through nominee or corporate directors, legal persons or legal arrangements splitting company incorporation and asset administration 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.*

Attractiveness of shell and shelf companies to criminals

A shell company or entity is a company which serves as a vehicle for business transactions without itself having any significant assets or operations. Shell companies are not in themselves illegal and they do have legitimate business purposes. Shelf companies are 'readymade' or 'off the shelf' companies that have often been acquired by a service provider such as a TCSP or Legal Practitioner, who holds the company with the aim of selling same in future. Shell and Shelf companies are also known as 'aged corporations', implying entities in existence for longer period. Some clients or entities may legitimately require to enable immediate trading, without prolonged business registration processes. Using a shell or shelf company promotes a long-standing image and prestige which buys social trust as a reliable entity, which has been long in existence and is not a 'fly by night'.

The fastness with which criminals can access such a corporate vehicle increases risks. In the so-called Fishrot case, shelf companies may have been used to receive bribes and other payments for the benefit of implicated government officials and their associates. The findings around legal persons' vulnerabilities can help inform prioritization or risk ratings for Legal Practitioners.

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. Below are a few examples worth looking out for:*

- *Clients who appear to actively and inexplicably avoid face-to-face meetings or who provide instructions intermittently without legitimate reasons and are otherwise evasive or very difficult to reach, when this would not normally be expected;*
- *Clients who appear to be acting on somebody else's instructions without disclosing the identity of such person. In particular, when a client requests services that can hide the true shareholders or directors of entities from competent authorities, the risk is higher with such client;*
- *Subsequent lack of contact, when this would normally be expected; and*
- *When the actual management of any trustee, company or legal entity appears to be acting according to instructions of unknown or inappropriate person(s).*

d. Use of Nominees: *Namibia's Mutual Evaluation[12] 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. Situations where a nominee is being used (e.g friend or family member is named as owner of property/assets where it is clear that the friend or family member is receiving instructions from the beneficial owner), with no apparent legal, tax, business, economic or other legitimate reason is high.*

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;

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

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;*

v. *the 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.*

Profile Mismatch

At times, the profile of the client might not match the values of funds client transactions in. In the single case of potential terrorism and TF investigated by NamPol, it was found that the primary suspect, a local Namibian, formerly Christian, who converted to Islam some years ago and became radicalized was sending funds to various high risk jurisdictions. Upon investigations, it was found that the suspect who send such via ADLAs/Money Service Businesses (MSBs), did not have the means to earn such funds, judging by his lifestyle audit revelations.

He was granted minority stake in two CCs. In one, he has shareholding of 5% and in another, he has shareholding of 10%. One entity is a 'car wash' and the other is a used car dealership. He appears to be a front man for foreign nationals from Kenya and Somalia, who are also closely associated with his faith. He appears to have been used by others to remit funds on their behalf as his earning and lifestyle did not suggest all the funds he was sending was his. The said primary suspect openly supports extremism and his activities on social media revealed same.

(Observations from the 2023 NRA update on TF)

e. ***High Risk Intermediaries:*** *Clients using financial intermediaries, financial institutions or legal professionals that are not subject to adequate AML/CFT laws and measures and that are not adequately supervised by competent authorities/regulatory bodies;*

f. ***False Information (or evasiveness):*** *when the person giving instructions to the Legal Practitioner is reluctant to provide all the relevant information or the Legal Practitioner has reasonable grounds to suspect that the provided information is incorrect or insufficient. This could include:*

- *Clients who have funds that are obviously and inexplicably disproportionate to their circumstances (e.g. their age, income, occupation or wealth);*
- *Clients who change their settlement or execution instructions without logical/appropriate explanation;*
- *Reluctance (or unconvincing explanation) to explain source of funds. If a customer or persons closely connected to him/her (or the counterparties) are unable or reluctant to provide correct information about the source of funds/wealth when this is requested. This could arise when there is a large and unexpected increase in the buyer's financial position and the buyer cannot explain the reason for their increased funds;*
- *Clients who change their means of payment for a transaction at the last minute and without justification (or with suspect justification), or where there is an unexplained lack of information or transparency in the transaction. This risk extends to situations where last minute changes are made to enable funds to be paid in from/out to a third party; and*
- *Clients who have no address, or who have multiple addresses without legitimate reasons.*

g. ***Known convicts or persons charged with proceed generating crimes:*** *Clients with previous convictions for crimes that generated proceeds, who instruct Legal Practitioners (who in turn have knowledge of such convictions) to undertake specified activities on their behalf. Clients associated with adverse/negative media reports as being linked to financial crimes are naturally high-risk;*

h. Client with links to high geographic risks: *Client companies that operate a considerable part of their business in or have major subsidiaries in countries that may pose higher geographic risk;*

i. Cash Intensive Clients: *Clients that are cash (and/or cash equivalent) intensive businesses. Where such clients are themselves subject to and regulated for a full range of AML/CFT requirements consistent with the FIA, this will aid to mitigate the risks; Conversely, clients or businesses that while not normally cash intensive appear to have substantial amounts of cash in their dealings with Legal Practitioners. Legal Practitioners thus need to understand the payment means of clients as banks will not often have the client financial profile when paying into trust accounts of practitioners;*

j. Politically Exposed Persons (PEPs) [13] ***:*** *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* [14] *be effectively or readily verified with relevant domestic authorities. PEPs need to be subjected to Enhanced Customer Due Diligence (EDD) which include obtaining management approval before facilitating deals involving them, as per FIC Guidance Note 01 of 2019;*

k. 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, Legal Practitioners need to be reasonably cautious and if need be, conduct enhanced due diligence with high networth clients;*

[13] 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.

[14] 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.

l. ***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.*

- *Clients who insist, without adequate justification or explanation, that transactions be effected exclusively or mainly through the use of virtual assets for the purpose of preserving their anonymity; and*
- *Generally, if a client appears to be involved in the cryptocurrencies space, additional care should be taken to duly understand their financial profile and source of funds.*

m. ***Risks associated with services NPOs:*** *NPOs engaging in transactions for which there appears to be no logical economic purpose or where there appears to be no link between the stated activities/objectives of the organization and the other parties in the transaction. The 2020 NRA found Faith Based Organisations (FBOs) to be most vulnerable to TF domestically. The 2023 NRA Update found NPOs involved in charitable services as highly exposed to TF abuse. Legal Practitioners are therefore reminded that FBOs and charities generally present increased TF risks. Worth noting is that domestically, FBOs have also been greatly abused to advance ML activities;*

n. ***Inexplicable or unreasonable ownership changes:*** *changes in ownership increase risk exposure to the Legal Practitioner availing relevant services in the process. 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), risk exposure is enhanced;*
- *Frequent or unexplained change of professional adviser(s) or members of management of the trustee, company or other legal entity;*

- *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.*

o. ***Indications of non-compliance:*** *Indicators that client does not wish to obtain necessary governmental approvals/filings, etc. This may include clients seeking to obtain residents rights or citizenship in the country of establishment of the TCSP in exchange for capital transfers, purchase of property or government bonds, or investment in corporate entities also increase risk exposure;*

p. ***Questionable or suspect business activities:*** *Clients who are suspected to be engaged in falsifying activities through the use of false loans, false invoices, and misleading naming conventions;*

q. ***Undue pressure:*** *Clients who request that transactions be completed in unusually tight or accelerated timeframes without a reasonable explanation for accelerating the transaction, which would make it difficult or impossible for the legal professionals to perform a proper risk assessment;*

r. ***Misalignments in proposed and actual activities:*** *when actual/real activities of the trust, company or other legal entity are unclear or different from the stated purposes under trust deeds, incorporation documents or internal regulations of the company or foundation, risk exposure is increased.*

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 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.

9.2.2 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. ***No concerns around prices unreasonably higher than valuation:*** *Property or Company/entity sales at prices that are significantly above or below market price, or 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. The Legal Practitioner must clearly understand the reasons for their customer's willingness to pay unusually higher prices;*

b. ***Unusually high offer for Legal Practitioners services:*** *The offer by the person giving instructions to the Legal Practitioner to pay extraordinary fees for services, which would not ordinarily warrant such a premium. Risks are also increased when payments are received from un-associated or unknown third parties and payments for fees in cash where this would not be a typical method of payment;*

c. ***Type of services required vs client profile:*** *residential or commercial, vacant land, investment, high-turnover properties, multi-unit properties for lettings/leases. An assessment needs to be made whether the client profile fits the proposed services. At times, the asset, share or investment value would not be in line with the profile of the customer. There are some conveyancing transactions wherein the client or buyer's financial profiles do not match the financial transactions they got into. Many a times, such indicates clients being used as fronts by others and may be suspicious;*

d. ***Attempts to unduly use the trust account for client payments:*** *Services that allow clients to deposit/transfer funds through the legal professional's trust account that are not tied to a transaction for which the Legal Practitioner is performing or carrying out activities. This also includes* ***client requests for irregular use of trust account such as*** *where the client may request financial transactions to occur outside of the legal professional's trust account (the account held by the legal professional for the client), e.g through the firm's general account and/or a personal or business account held by the legal professional himself/herself;*

e. ***Requests to hide shareholders/owners:*** *Services where the legal professional acts as a trustee/director that allows the client's identity to remain anonymous;*

f. ***Irregular patterns:*** *Payments received from un-associated or unknown third parties and payments in cash where this would not be a typical method of payment;*

g. ***Cash:*** *Customers making cash payments are inherently presenting higher ML/TF/PF risks. Cash in this instance refers to all payments for services (or for entity acquisitions, shares etc) not financed by financial institutions (e.g loans). Legal persons or individuals from cash intensive businesses present a higher risk. 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.* ***This naturally also implies that clients funded through loans present lower risks as their sources of funds can be traced to Financial Institution loans. Lower risk clients should not be subjected to EDD. This not only creates inefficiencies but increase compliance efforts and costs;***

h. ***Use of pooled client funds/accounts or safe custody:*** *Pooled client funds or assets, without justification or legitimate business reasons often increases risk as funds could be pooled from illegitimate sources;*

i. ***Bearer shares[15]:*** *"Bearer shares are not prohibited in Namibia in terms of sections 107 and 110(4) of the companies act 2004 as amended 2007. Further, no legal provisions exist for immobilizing bearer shares and share warrants by requiring them to be held with a regulated financial institution or professional intermediary, found the Mutual Evaluation on Namibia[16]. Bearer shares represent increased ML/TF/PF risk;*

j. ***Use of multiple accounts:*** *When client uses multiple accounts 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, Legal Practitioners 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;*

k. ***Unusual activities:*** *Unusually high levels of assets or unusually large transactions compared to what might reasonably be expected of clients with a similar profile may indicate that a client not otherwise seen as higher risk should be treated as such. Legal Practitioners' risk exposure is also increased around clients that start or develop an enterprise with unexpected profile or abnormal business cycles or clients that enter into new/emerging markets. Organised criminality generally does not have to raise capital/debt, often making them first into a new market, especially where this market may be retail/cash intensive;*

l. ***Uncommon trend(s):*** *The relationship between employee numbers/structure is divergent from the industry norm (e.g. the turnover of a company is unreasonably high considering the number of employees and assets compared to similar businesses). Similarly, the following should be considered high risk:*
   - *The postponement of a payment for an asset or service delivered immediately to a date far from the moment at which payment would normally*

[15] In simple, terms, a bearer share is equity security wholly owned by the person or entity that holds the physical stock certificate, thus the name "bearer" share. The issuing firm neither registers the owner of the stock nor tracks transfers of ownership; the company disperses dividends to bearer shares when a physical coupon is presented to the firm. Because the share is not registered to any authority, transferring the ownership of the stock involves only delivering the physical document.

[16] See Page 171, Under Recommendation 24, Criterion 24.11.

be expected to occur, without appropriate assurances that payment will be made is risky; and

- *Successive capital or other contributions in a short period of time to the same company with no apparent legal, tax, business, economic or other legitimate reason.*

m. Unexpected resuscitation: *Sudden activity from a previously dormant client without a clear explanation;*

n. Late changes to methods/transacting activities: *Clients who change their means of payment for a transaction at the last minute and without justification (or with suspect justification), or where there is a lack of information or transparency in the transaction. This risk extends to situations where last minute changes are made to enable funds to be paid in from/out to a third party;*

o. No apparent reason for using your Legal Services: *Significant and unexplained geographic distance between the Legal Practitioner and the location of the customer is inherently a red flag until proven otherwise. Legal Practitioners should carefully consider the nature of the business relationship or transaction with client. For example, where the scale of the transaction or location of the proposed business suggests that another Legal Practitioner (or method) would have been better placed to facilitate the deal, avail such services etc., you should consider carefully why the customer chose your business. Illogical patterns may indicate efforts to lower the risk of detection (e.g. if the same customer is making other transactions with other Legal Practitioners more accessible or local to them but does not want the scale of their activity known) or collusion between Legal Practitioners and the beneficial owner(s);*

p. Misuse of Legal Practitioner advise: *This may be difficult to detect at first. Situations where advice on the setting up of legal persons or legal arrangements may be misused to obscure ownership or real economic purpose (including setting up of trusts, companies or other legal entities, or change of name/corporate seat*

or establishing complex group structures). This might include advising in relation to a discretionary trust that gives the trustee discretionary power to name a class of beneficiaries that does not include the real beneficiary (e.g. naming a charity as the sole discretionary beneficiary initially with a view to adding the real beneficiaries at a later stage). It might also include situations where a trust is set up for the purpose of managing shares in a company with the intention of making it more difficult to determine the beneficiaries of assets managed by the trust;

q. Attempts to facilitate, advance, support or commit illicit activities: *Any attempt by the proprietor, representative, beneficial owner, trustee, company or other legal entity to enter into any arrangement to fraudulently evade tax or advance ML and TF in any relevant jurisdiction;*

r. Request to vouch on behalf of client: *Services where Legal Practitioners may in practice represent or assure the client's standing, reputation and credibility to third parties, especially without a commensurate knowledge of the client's affairs could help legitimise potential dodgy beneficial owners or dealings. In the same vein, when Power of Representation/Attorney is given in unusual conditions (e.g. when it is granted irrevocably or in relation to specific assets) and the stated reasons for these conditions are unclear or illogical, risks are increased;*

s. Unreasonable granting of power of representation: *Power of representation given in unusual conditions (e.g. when it is granted irrevocably or in relation to specific assets) and the stated reasons for these conditions are unclear or illogical;*

t. Transactions involving closely connected persons *and for which the client and/or its financial advisors provide inconsistent or irrational explanations and are subsequently unwilling or unable to explain by reference to legal, tax, business, economic or other legitimate reason;*

u. Illogical acquisition of entity in liquidation: *Acquisitions of businesses in liquidation with no apparent legal, tax, business, economic or other legitimate*

reason increases risks. Generally, Legal Practitioners need to be able to identify when commercial, private, or real property transactions or services are to be carried out by the trust, company or other legal entity with no apparent legitimate business, economic, tax, family governance, or legal reasons. Attempts to avoid lawful interventions in ownership immediately before lawful restraint or insolvency are a high risk;

v. ***Irregular/uncommon payment methods:*** *Part or full settlements in cash, cleared funds or foreign currency, with unconvincing reasons. This could indicate laundering of cash proceeds of crime, tax evasion, or to avoid insolvency or an order to recover property. Further, the use of irregular or complex financial, equity, investment or loans transactions can be an option to obscure criminal activities;*

w. ***Known suspicions:*** *Existence of suspicion of fraudulent transactions, or transactions that are improperly accounted for increase risks. These might include:*
   - *Over or under invoicing of goods/services;*
   - *Multiple invoicing of the same goods/services;*
   - *Falsely described goods/services – over or under shipments (e.g. false entries on bills of lading); and*
   - *Multiple trading of goods/services.*

x. ***High Risk TCSP services:*** *Legal Practitioners who offer TCSP services should have regard to this Guidance[17], and should consider customer or service risks related to TCSPs such as the following:*
   - *Unexplained delegation of authority by the client through the use of powers of attorney, mixed boards and representative offices;*
   - *Provision of registered office facilities and nominee directorships without proper explanations; and*
   - *Unexplained use of discretionary trusts.*

[17] Along with FIC Guidance Notes 05 and 06 of 2023, accessible on the FIC website at: https://www.fic.na/index.php?page=2023-guidance-notes

9.2.3 Considering Country or Geographic risk

There is no universal standard of what a high risk jurisdiction within the AML/CFT/CPF framework is. Best practices, noted from the FATF[18], 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. The NRAs and Sectoral Risk Assessments (SRAs) observe that Legal Practitioners attract foreign clients from all over the world. Some from countries without reliable identification infrastructure. There is a possibility that such clients could be linked to complex and opaque legal structures internationally, a factor which may enhance 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[19] states. Information about high-risk jurisdictions is widely available, which is detailed from several open-source documents and media. 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 having in place ineffective AML/CFT/CPF measures;*
    - *identified to be uncooperative in extraditions and providing beneficial ownership information to competent authorities, a determination of which may be*

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

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

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;

- *or areas identified by credible sources as providing funding or support for terrorist activities or that have identified/designated 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;*
- *subject to sanctions or embargoes issued by international community including the UN, OFAC, EU etc; and*
- *having terrorist organisations designated by the UN, US, EU, other countries, and international organisations.*

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 Legal Practitioners' 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.

9.3 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 Legal Practitioner (or fellow practitioners along the value chain/in the deal/transaction). If such partnership exists, the Legal Practitioner 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).

9.4 Type, Nature and Extent of Controls

To reduce inherent[20] risks to tolerable or acceptable residual[21] levels Legal Practitioners have a responsibility to implement controls and duly demonstrate their effectiveness to authorities such as the FIC. The FIC 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.

9.5 External Risk Assessments

The considerations and indicators herein are not extensive. Legal Practitioners are required to consider observations from SRAs and NRAs issued by the FIC. Local[22] and international trends and typology reports issued by bodies such as ESAAMLG[23] and FATF[24] (available on their websites) equally help highlight changing risks broadly and 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.

10. 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 Legal Practitioners. Legal Practitioners are further required to duly study Guidance Note 15 of 2023 which speaks to the practical implementation of controls to mitigate ML/TF/PF risks at institutional level.

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

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.

11. 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.

12. NON-COMPLIANCE WITH THIS GUIDANCE

This document is a guide. Effective implementation is the sole responsibility of Legal Practitioners. 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: 05 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