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. 15 OF 2023

GUIDANCE ON THE IMPLEMENTATION OF RISK BASED CONTROLS AND REPORTING SUSPICIONS:

LEGAL PRACTITIONERS AND LAW FIRMS

First Issued: 05 July 2023

TABLE OF CONTENTS

DEFINITIONS AND ABBREVIATIONS

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

"Beneficial Owner"[1] refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement;

"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;

[1] FATF RBA on TCSPs, June 2019. file:///C:/Users/ham638/Downloads/RBA-Trust-Company-Service-Providers%20(5).pdf

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

"ML" means Money Laundering;

"Monitoring" as defined in the FIA, for purposes of Sections 23, 24 and 25 of the Act includes -

a. the monitoring of transactions and activities carried out by the client to ensure that such transactions and activities are consistent with the knowledge that the accountable institution has of the client, the commercial or personal activities and risk profile of the client;
b. the enhanced monitoring of transactions and activities of identified high risk clients in order to timeously identify suspicious transactions and activities; and
c. the screening of the name of a client or potential client, and the names involved in transactions, against the sanctions lists issued by the United Nations Security Council under Chapter VII of the United Nations Charter; for purposes of combating money laundering, the financing of terrorism and the funding of proliferation activities.

"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;

“SNMA” refers to a Sanction Name Match Activity Report. When a potential sanctions match is detected, institutions should file a SNMA with the FIC. With effect from 17 April 2023, all sanctions name matches should be reported through SNMA reports and no longer through STRs or SARs;

“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;

“TPFA” means Terrorist & Proliferation Financing Activity report. Reporting any other Activity (or attempted transaction which was not completed) which may point to, or be linked to potential terrorism, TF or PF;

“TPFT” means Terrorist & Proliferation Financing Transaction report. Reporting any other Transaction (actual transaction that has taken place) which may point to, or be linked to potential terrorism, TF or PF;

“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 trusts and legal persons. Some Accountants, Legal Practitioners and Financial Institutions also provide these services;

“Without delay” means taking required actions within a few hours, as advised in Namibia’s September 2022 Mutual Evaluation Report.

1. BACKGROUND

This Guidance Note is issued in terms of Section 9(1)(h) of the Financial Intelligence Act, 2012 (The FIA). It is the second part of two sectoral guidance notes for all Legal Practitioners and law firms that avail designated services as per Schedule 1, Item 1 and 3 of the FIA. Such services in essence are those related to the buying and selling of real estate; creation and transfer of interests in legal persons, trusts, partnerships and such similar arrangements as well as management of client funds/investments in relation to such services. This guidance note applies to all such Legal Practitioners and law firms. In the context of this guidance note, the reference to Legal Practitioners includes sole proprietors or one-man practitioners, law firms and all persons duly recognised[2] to avail such services regardless of how they identify themselves.

Legal Practitioners, like all other sectors are required to adopt a Risk Based Approach (RBA) in their overall management of risks they are exposed to. The RBA starts with conducting risk assessments at institutional level, which includes observations from Sectoral and National Risk Assessments, amongst others. Guidance Note 14 of 2023 guides how Legal Practitioners should conduct risk assessments while this specific Guidance Note (15 of 2023) explains how Legal Practitioners should implement controls which are informed by outcomes of such risk assessments.

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. In an effort to 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, at institutional level.

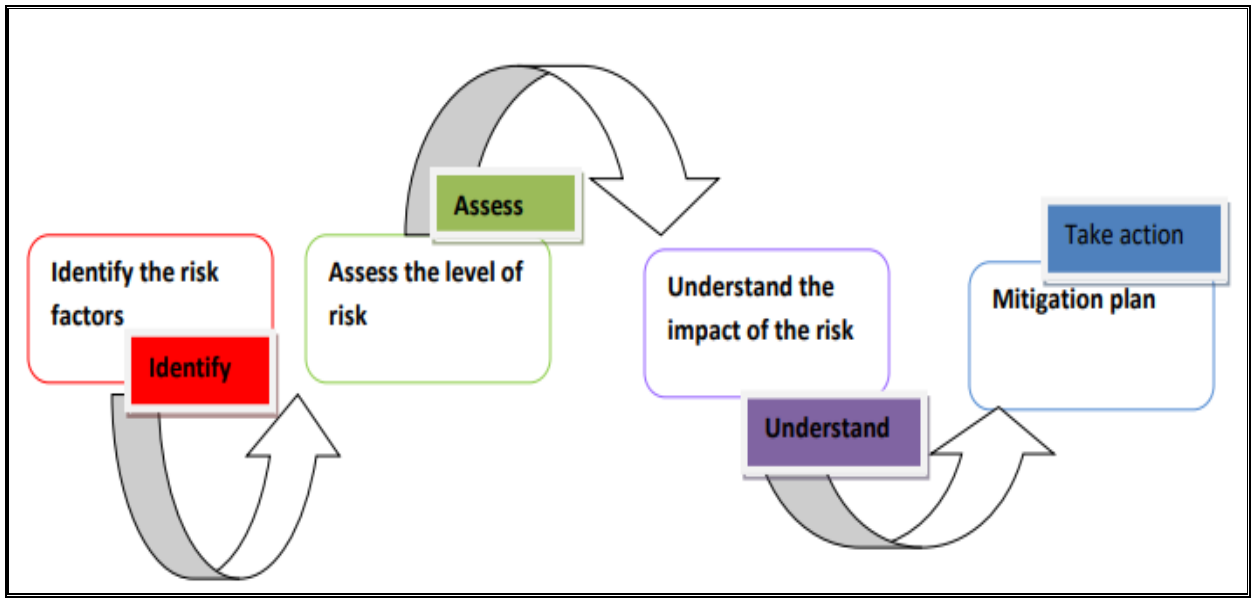
2. COMMENCEMENT

This Guidance Note comes into effect on **06 July 2023**.

[2] As per the Legal Practitioners Act, 1995 (Act No. 15 of 1995).

3. THE RISK BASED APPROACH (RBA)

As explained in Guidance Note 14 of 2023 and other FIC publications, the RBA speaks to a control system premised on a Legal Practitioner's understanding of risks it may be exposed to. Such understanding is what informs the design, nature and extent of controls implemented to mitigate risks (mitigation plan). See diagram below. The key features are identifying and assessing 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

As mentioned above, Guidance Note 14 of 2023 deals with the identification and assessment or evaluation of risks (and high risk indicators) presented by customers/clients and the vulnerability of services or transactions related to such. This Guidance Note uses an understanding of sectoral risks and avail considerations Legal Practitioners should take into account when implementing risk-based controls to combat ML, TF and PF risks. The guidance herein focuses on primary

controls such as: effecting appropriate CDD[3] measures for customers; on-going and enhanced due diligence of client behaviour[4]; record keeping[5] to assist criminal investigations; monitoring[6] to detect suspicions and reporting[7]. The FIC website[8] contains Directives, Guidance Notes, Circulars and Regulations which avail helpful guidance on measures to combat ML/TF/PF in terms of the FIA. Below are simplified considerations Legal Practitioners may start with, in implementing a RBA.

3.1 Practical Starting Point

Legal professionals and law firms must protect themselves from unwitting involvement in ML/TF. Such involvement not only presents reputational risk to the individuals concerned, but the law firm and the legal profession at large, the social trust and confidence that society has in the legal profession can be eroded if the legal profession allows itself to be misused by criminals. Legal professionals should perform a risk assessment of the client at the inception of a client relationship.

A practical starting point for Legal Practitioners and law firms would be to take the following approach[9]:

a) **Client acceptance and know your client policies:** identify the client and its beneficial owners and the true "beneficiaries" of the transaction. Obtain an understanding of the source of funds and nature or source of income or wealth of the client where required, its owners and the purpose of the transaction. This is needed to enable comparisons of when transacting values or behaviour is outside the client's financial profile;

[3] FIA Sections 21 and 22
[4] FIA Sections 23 and 24
[5] FIA Sections 26 and 27
[6] FIA Section 24
[7] FIA Section 33
[8] https://www.fic.na/index.php?page=publications
[9] Many of these elements are critical to satisfying other obligations owed to clients, such as fiduciary duties, and as part of their general regulatory obligations.

b) **Engagement acceptance policies:** understand the nature of the work. Legal Practitioners should know the exact nature of the service that they are providing and have an understanding of how that work could facilitate the movement or obscuring of the proceeds of crime. Where a Legal Practitioner does not have the requisite expertise, the Legal Practitioner should not undertake the work as he or she will not the required expertise to ensure risk mitigation and thus compliance with the FIA;

c) **Understand the commercial or personal rationale for the work:** Legal Practitioners need to be reasonably satisfied that there is a commercial or personal rationale for the work undertaken. They however are not obliged to objectively assess the commercial or personal rationale if it appears reasonable and genuine;

d) Be **attentive to red flag indicators:** exercise vigilance in identifying and then carefully reviewing aspects of the transaction if there are reasonable grounds to suspect that funds are the proceeds of a criminal activity, or related to terrorist financing. Subject to qualifications set forth in this Guidance[10], these cases would trigger reporting obligations. Documenting the thought process may be a viable option to assist in interpreting/assessing red flags/indicators of suspicions;

e) Then consider what action, if any, needs to be taken and **have an action plan:** the outcomes of the above action (i.e the comprehensive risk assessment of a particular client/transaction) will dictate the level and nature of the evidence/documentation collated under a Legal Practitioner or firm's CDD/EDD procedures (including evidence of source of wealth or funds); and

f) **Documentation:** legal practitioners should adequately document and record steps taken under a) to e).

[10] And other Guidance Notes including Guidance No. 05, 07 and 14 of 2023, available on the FIC website. https://www.fic.na/index.php?page=publications

3.2 Framework for RBA

The elements highlighted below support practical control measures listed above. Subject to the size and scope of the Legal Practitioner (or law firm), the framework of risk-based internal controls should:

a) have appropriate risk management systems to **determine the risk level of a client, potential client, or beneficial owner**;

b) following from the above, provide for **effective controls for higher risk clients and services as necessary** (e.g additional due diligence, obtaining information on the nature and source of wealth and funds of a client, escalation to senior management or additional review and/or consultation by the Legal Practitioner or within a law firm);

c) provide **increased focus on a Legal Practitioner's operations** (e.g services, clients and geographic locations) that are **more vulnerable to abuse** for ML/TF;

d) provide for **periodic review of the risk assessment and management processes**, taking into account the environment within which the legal professional operates and the services it provides;

e) designate personnel at an appropriate level **who are responsible for managing AML/CFT compliance**;

f) provide for an **AML/CFT compliance function and review programme** as appropriate given the scale of the organisation and the nature of the legal professional's practice; and

g) implement **risk-based CDD policies, procedures and processes**, including review of client relationships from time to time to determine the level of ML/TF risks;

h) incorporate **AML/CFT compliance into job descriptions** of relevant personnels;

i) implement a **documented program of ongoing staff AML/CFT awareness and training**. This should include policies and procedures to ensure staff awareness around their role and responsibilities in filing suspicions reports with the FIC;

j) The most effective tool to monitor the internal controls is a **regular** (typically at least annually) **independent compliance review**. The review can be internal or external. If carried out internally, a staff member who may have a good working knowledge of the law firm's AML/CFT internal control framework, policies and procedures and is sufficiently senior to challenge them should perform the review. The person conducting an independent review should not be the same person who designed or implemented the controls being reviewed. The compliance review should include a review of CDD documentation to confirm that staff properly apply the law firm's procedures[11]; and

k) Depending on risk exposure and size of transactions, amongst others, Legal Practitioners should **consider using reputable technology-driven solutions**[12] to minimise the risk of error and find efficiencies in their AML/CFT processes. As these solutions are likely to become more affordable, and more tailored to the legal profession as they continue to develop, this may be particularly grow in importance for smaller law firms that may be less able to commit significant resources of time to these activities.

Sections 4 to 11 herein below avails detailed and practical guidance on the implementation of the above.

[11] The FIA obligation in this regard (section 39) is informed by the FATF Recommendations. See Guidance for a Risk-Based Approach: Legal Professionals, June 2019. file:///C:/Users/ham638/Downloads/Risk-Based-Approach-Legal-Professionals.pdf

[12] As per the FIA and FATF Recommendation 17, the ultimate responsibility for CDD measures should remain with Legal Practitioners relying on the technology-driven solutions utilized.

4. EXTENT OF CUSTOMER DUE DILIGENCE MEASURES

The nature and extent of CDD measures a client ought to be subjected to depends on the degree of risk that such individual client, in view of the transaction, presents to the Legal Practitioner.

CDD goes beyond simply carrying out identity checks to obtain names and identification numbers. The object of CDD is to build a client profile. This is important because even people known to the Legal Practitioner may become involved in illegal activities at some point, for example, if their personal circumstances change or they face new financial pressures. The Legal Practitioner should be able to demonstrate that the extent of the CDD measures applied for each client are appropriate to mitigate risk exposure arising from such client. With selling of companies or other legal entities, Legal Practitioners should bear in mind that there is likely to be different levels of risk between buyers and sellers in general as both sides are participating in a financial transaction, either by releasing finance from a property (or other investment) they already own, or by introducing purchase funds.[13]

4.1 Simplified Due Diligence

The below explains simplified CDD for natural persons when they access Legal services in their personal capacities. Such is also applicable for natural persons when they act on behalf of legal persons such as Close Corporations or Companies and such arrangements like Trusts or partnerships.

4.1.1 Extent of Simplified CDD

The extent to which simplified CDD should be applied is essential to financial inclusion objectives. For this reason, such due diligence should not be extensive if all relevant considerations indicate a low risk. FIA Regulations 6 to 11 provide guidance on the minimum identification procedures that should be followed for the various types of clients. The guidance herein builds on same.

[13] RBA Guidance for Real Estate Agents, FATF (2008)

4.1.2 Ascertainment and Verification of Information: Natural Persons

Simplified CDD is the first level of due diligence applied when the risk is minimal. When simplified CDD is applicable, Legal Practitioners are still required to identify and verify or ascertain customers' identification information. Below is a list of the type of information which needs to be ascertained/verified and that which needs to be obtained (from client):

a. Verification: full names;
b. Verification: nationality;
c. Verification: If citizen – national ID no./ passport no./date of birth;
d. Verification: Non-citizen – passport no./national ID no./date of birth;
e. Obtain: Namibia residential address for citizens OR if non-citizen, residential address in his/her country or physical address in Namibia, if any; and
f. Contact particulars.

Legal Practitioners need to ensure due verification of identification information before availing any services. Verification should ideally be done with the Ministry of Home Affairs' National Identification Database. However, such is not possible at the time of issuing this guidance. Legal Practitioners should thus use other reliable means to verify identify of clients such as comparing ID documents to passports, driver's license cards, voter's cards, birth certificates and such other reliable mechanisms.

4.1.3 Tips on simplified CDD

Legal Practitioners may:

a. use information already at hand such as client profile, without unduly requesting for more. For example, if you identified your customer as a Manager in a local shop or Pensioner, you can assume what the source of funds is, unless other factors exist (such as higher financial values which may be beyond reasonable earnings of Manager or Pensioner); and
b. adjust the frequency of CDD reviews when necessary, for example, when a change occurs which may suggest escalation of the low-risk behaviour.

4.1.4 Pre-requisites for Simplified Due Diligence

To apply simplified CDD, a Legal Practitioner must ensure:

a. it is supported by internal customer risk assessment;
b. enhanced due diligence does not apply (there is no high risk in terms of client, nature of transaction/service or geographic considerations etc.);
c. monitoring the business relationship or transactions (e.g with frequent transactions of similar client) to ensure that there is nothing unusual or suspicious from the outset;
d. customer is not from, nor associated with a high risk country;
e. the customer is not a PEP, a family member, or a known close associate of a PEP;
f. the real customer is seen face-to-face (and not having others transact on his/her behalf unreasonably to evade detection);
g. customer is not accessing or desiring to acquire/take over a shell or shelf company;
h. client is not trying to deliberately create a complex structure to hide the identification of true beneficial owners or those who will ultimately control the trust or company;
i. the source of funds or wealth are transparent and understood; and
j. the transaction is not complex or unusually large.

Guidance Note 14 of 2023 avails detailed guidance on how to assess the risk level emanating from transactions or clients and equally lists indications of high risk.

4.1.5 When to cease Simplified CDD and commence EDD:

Generally, the FIA requires Legal Practitioners to commence EDD when the risk level is escalated from low to medium and especially high. Below are a few examples:

a. If suspicions of ML, TF or PF arise;
b. doubt whether documents obtained for identification are genuine;
c. doubt whether the customer is indeed the one demonstrated in the documentation;
d. indications that client may be transacting on behalf of another unduly (or when there are attempts to hide identification of some or all beneficial owners);

e. The structure or nature of the entity or relationship makes it difficult to identify the true owner or those directing affairs behind the scenes. Be careful of true owners or directors who do not wish to be recorded on company or trust documents. They usually present high ML, TF, PF risks. For example, checks can be done via BIPA, local authorities, Deeds offices etc., to ascertain certain information. If a customer seeking to buy a property is a corporate vehicle and you cannot identify the ultimate beneficial owner, you should:
   - keep records in writing of all the actions taken to identify the ultimate beneficial owner of the body corporate; and
   - take reasonable measures to verify the identity of the senior person in (or associated with) the entity responsible for managing it and keep records in writing of the actions taken to do so, and any difficulties encountered. Consider carefully the risks associated with beneficial owners as per Guidance 14 of 2023 and various other publications.

f. suspect that the documents obtained for identification maybe lost, stolen or otherwise fraudulently acquired. Impact of identity theft is rife especially with online activities or non-face-to-face clients;

g. circumstances change and your risk assessment no longer considers the customer, transactions, or location as low risk; and

h. Any other considerations that do not maintain the low risk of client or specific transaction(s).

Guidance Note 14 of 2023, especially section 9.2, avails detailed guidance on transactions or clients who may present higher risks. Such should be duly considered.

5. ENHANCED DUE DILIGENCE (EDD)

It is critical that a Legal Practitioner has measures that can identify when to escalate from simplified CDD to EDD, e.g identifying that a client meets the definition of a PEP. EDD applies when a client's risk profile or transaction is not low. It includes taking additional measures to identify and verify customer identity, creating a client's financial profile including the source of funds and conducting additional ongoing monitoring. The EDD measures in this section apply to Legal Practitioners' clients who are natural, unless otherwise indicated. The section below expands on such EDD measures.

5.1 Nature and Type of EDD Measures

It is essential to keep in mind that identification procedures as per FIA Regulations 6 to 11 regulate obtaining the minimum identification information or simplified CDD while Regulation 12 provides for EDD or obtaining additional information[14] when higher risks arise. EDD means building onto the basic identification information obtained as per simplified due diligence measures in parts 4.1.1 and 4.1.3 above. Such EDD information, for natural persons, primarily includes the following and is useful in monitoring transactional behaviour:

Type of EDD Information	Usefulness of Such
Nature & location of business activities	Creating client financial profile: Helps Legal Practitioners create context around magnitude of clients' earning capabilities, especially for self-employed or businesspeople.
Occupation or source of income	
Source of funds involved in transaction	Enables a comparison of transacting behaviour through funds to be used vs the profile of the customers.

This should be clearly outlined in the AML/CTF/CPF policies, procedures and internal controls of the Legal Practitioner.

5.2 When to undertake EDD

i. As per internal risk assessment, a Legal Practitioner has determined that there is a high risk of ML, TF or PF associated with the client or transaction;
ii. FIC or another supervisory or law enforcement authority provides information that a particular situation or client is high risk;
iii. a customer originates from or has ties to a high risk country;
iv. client is evasive, has given you false or stolen documents to identify themselves (immediately consider reporting this to FIC as suspicious transaction/activity);

[14] the extent of which is dependent on the risk the client/transaction may pose to the ADLA.

v. a customer is a Politically Exposed Person (PEP), an immediate family member or a close associate of a PEP;
vi. the transaction is complex, or unusually large, or with an unusual pattern and have no apparent legal or economic purpose;
vii. client deposits or introduces funds with the Legal Practitioner and soon thereafter, without logical explanation, chooses to withdraw from transaction and asks for a transfer/refund;
viii. client refusing to continue with transaction when asked to avail EDD information; and
ix. Any other considerations enhancing client or transaction risk.

Guidance Note 14 of 2023 avails detailed guidance on clients, activities, transactions, delivery channels and circumstances that present high risks. Such should be duly considered.

5.3 The concept of additional measures in EDD

For EDD to be undertaken duly, the Legal Practitioner must do more to verify, identify and scrutinise the background and nature of clients and their relevant conduct. This is usually more extensive than simplified CDD measures. The extent to which EDD goes beyond simplified CDD must be clearly stated in the Legal Practitioner's AML/CFT/CPF policies and procedures. For example, the Legal Practitioner should:

a. obtain additional information or evidence to establish the identity from independent sources, such as supporting documentation on identity or address or electronic verification alongside manual checks;
b. take additional measures to verify the documents supplied such as by checking them against additional independent sources, or require that copies of the customer's documentation are certified by a bank, financial institution, lawyer or notary who is competent at document inspection and impostor detection, or a person from a regulated industry or in a position of trust;
c. when receiving funds for the transaction or to manage on behalf of client (even if it is paid directly to your bank account), ensure such funds are being introduced by the client and not another person merely using a client to introduce funds in the deal;

d. the following measures must be taken when the transaction relates to a PEP, a family member or known close associate of a PEP (See Guidance Note 01 of 2019 on PEPs):
   - obtain senior management approval before establishing a business relationship with that person;
   - take adequate steps to establish their nature of business activities, source of wealth and actual source of funds introduced; and
   - conduct enhanced ongoing monitoring if transactions are frequent or appear structured.

e. carry out more scrutiny of the client's known (or accessible record of) transactions/conduct and satisfy yourself that it is consistent with the client profile;

f. measures which must be taken when a client originates from, or has ties to a high-risk main or third country[15]:
   i. Obtain additional information on the customer and the customer's beneficial owner(s), if they identify themselves as associated with a high risk entity;
   ii. Obtain the approval of senior management for establishing or continuing the business relationship; and
   iii. Where possible, e.g for ongoing relationships, enhance monitoring of the business relationship by increasing the number and timing of controls applied and select patterns of transactions which require further examination.

6. CDD RELATED TO LEGAL PERSONS, TRUSTS AND OTHER ARRANGEMENTS

While section 5 above focused on clients who are natural persons, this section outlines considerations as per the FIA when identifying legal persons, partnerships and trusts etc.

6.1 Ascertainment of information: Companies and Close Corporations (CCs)

Legal Practitioners are encouraged to keep in mind that CCs are the most abused entities in the advancement of ML locally, in terms of financial values as per the 2023 National Risk Assessment (NRA) Update. While companies may not be as highly exposed to risks as CCs, their vulnerability

[15] (a business is established in a country if they are incorporated there, is their principal place of business, or they are regulated there as a financial or credit institution; an individual is established in a country if they are resident there)

in terms of high level of their frequent abuse in cases still very high for comfort. It is essential that the following information is obtained, as a minimum, for identification purposes:

a) its **registered name;**
b) the **name under which it conducts business** in the country in which it is incorporated;
c) if the company or close corporation is incorporated outside of Namibia and conducts business in Namibia using a name other than the name specified under paragraph (a) or (b);
d) **the name used in Namibia**;
e) its **registration number**;
f) the **registered address** from which it operates in the country where it is incorporated, or if it operates from multiple addresses in that country the address of its head office;
g) **Ultimate Beneficial Owners (UBOs):** the **identification particulars for natural persons** who exercise **effective control** of the company or CC, as referred to in 4.1.2. The following are indications of such persons:
    i. the executive manager/s chief executive officer and beneficial owners of the company or, in the case of a close corporation, each executive manager/s, each member/s who individually or collectively holds a controlling interest and the beneficial owners;
    ii. each natural person who purports to be authorised to establish a business relationship or to enter into a transaction with the accountable or reporting institution on behalf of the company or close corporation; and
    iii. the identity of shareholders and their percentage ownership: from such, each natural person (member/shareholder) holding 20% or more of the voting rights at a general meeting of the company concerned or acting or purporting to act on behalf of such holder of such voting rights. **Legal Practitioners need to deliberately make efforts to identify any other persons, other than the stated owners/members, who may be exercising effective control or 'directing affairs' of the CC in the background, as stated in the next section below. Usually, the risk is higher when such persons are not recorded on relevant company or CC documents.**

    The obligation to identify beneficial ownership does not end with identifying the first level of ownership but requires reasonable steps to be taken to identify the

ownership at each level of the corporate structure until an ultimate beneficial owner is identified. A Legal Practitioner's AML/CFT/CPF policies and procedures must outline all such deliberate measures aimed at identifying the UBOs. See expanded explanations on EDD for UBOs in sections 6.1.1 - 6.1.2 below.

6.1.1 Ultimate Beneficial Ownership in CCs

Understanding the **ownership and control structure** of the client and gaining an understanding of the client's source of wealth and source of funds helps reduce risks of Legal Practitioners being abused to advance ML/TF/PF.

At the time of publishing this guidance, the Business and Intellectual Authority (BIPA) is in the process of sourcing all relevant ultimate beneficial ownership (UBO) information not in its possession and uploading same on an accessible portal which can be used by Accountable Institutions for verification as per the FIA. The ideal expectation is that all UBO information should be verified with relevant authorities such as BIPA.

Legal Practitioners should understand who the beneficial owners are from accessing CC incorporation documents. Beneficial ownership includes not only interest holders/shareholders but importantly those who exercise effective control such as Executive Management. CC incorporation documents reflect Members as the UBOs. If it becomes apparent, during the process of availing services that other persons not listed as such, exercise effective control which is ideally expected of members or owners, such person(s) should be duly identified and the Legal Practitioners should understand why such person(s) is not listed on the CC incorporation documents as a Member. If there are no logical explanations, the Legal Practitioner should file a STR/SAR with the FIC if ML is a possibility and TPFA or TPFT when TF or PF is suspected. The following can help indicate beneficial owners not listed on relevant incorporation documents:

a. profile of members may not be consistent with the nature of such business activities (e.g the members on incorporation documents may not appear to have an

understanding of the nature of business activities they are involved in or may not have the required capital to invest in such business); and

b. when the Legal Practitioner avails services, if it becomes apparent that members or those purporting to be such are having to consult or seek permission for matters they (as members) should be able to explain or take decisions on.

Some of the information listed under 6.1.2 below as sources for verification can also be used for CCs.

6.1.2 Ultimate Beneficial Ownership in Companies (including section 21 companies)

BIPA currently obtains information around the directors of companies. The Mutual Evaluation found that BIPA has not been obtaining information about the identification of the UBO such as shareholders. This creates challenges with verification requirements as per the FIA. Legal Practitioners, like all other Accountable Institutions need to access the company incorporation documents and request of relevant parties to the transaction to avail information such as share certificates which may confirm shareholder information. Other verification exercises can also be considered, such as enquiries with other Legal Practitioners, relevant Accountants and Auditors of such companies etc.

To verify the information listed above 6.1(g), Legal Practitioners may use the below measures:

a. **Financial profile of UBOs is helpful.** obtaining additional information on the beneficial owner or natural person exercising effective control of the trust, company or other legal entity (e.g. occupation, overall wealth, information available through public databases, internet), and updating more regularly the identification data of such persons and sources which can be regarded as credible;
b. obtaining information on the **reasons for intended or performed transactions** carried out by the company or other legal entity as per founding/constitutional documents (such as a certificate of incorporation, memorandum and articles of incorporation/association);

c. details from **company registers**;
d. shareholder **agreements** or other agreements between shareholders concerning control of the legal person;
e. EDD may also include **lowering the threshold of ownership** (e.g. below the stated 20%), to ensure complete understanding of the control structure of the entity involved;
f. looking **further than simply holdings of equity shares**, to understand the **voting rights** of each party who holds an interest in the entity; and
g. filed audited accounts.

6.1.3 Nominee Directors and Shareholders

The Mutual Evaluation report of Namibia observed as follows:

"Based on the circumstances of the Fishrot case, one area of huge risk which has not been determined to what extent it is prevalent is the abuse of shelf companies in the commission of serious crimes, ML included. BIPA did not demonstrate that after the Fishrot cases, it had proceeded to take reasonable steps to determine to what extent shelf companies were being abused to facilitate commission of serious crimes. Connected to the risks posed by shelf companies, are the risks associated with the use of nominee shareholders and nominee directors which still have not been assessed nor are they understood by the authorities. Further, the authorities did not demonstrate the measures which have been put in place that if there are any risks associated with the use of nominee shareholders and directors, these are assessed, understood and monitored as they evolve."

A nominee director is a person who has been appointed to the Board of Directors of the legal person who represents the interests and acts in accordance with instructions issued by another person, usually the beneficial owner. A nominee shareholder is a natural or legal person who is officially recorded in the Register of Members (shareholders) of a company as the holder of a certain number of specified shares, which are held on behalf of another person who is the beneficial owner. The shares may be held on trust or through a custodial agreement.

There are legitimate reasons for a company to have a nominee shareholder including for the settlement and safekeeping of shares in listed companies where post traded specialists act as nominee shareholders. However, in the AML/CFT/CPF framework, these nominee director and nominee shareholder arrangements can be misused to hide the identity of the true beneficial owner/s of the legal person. There may be individuals prepared to lend their name as a director or shareholder of a legal person on behalf of another without disclosing the identity of, or from whom, they will take instructions or whom they represent. They are sometimes referred to as "strawmen".

This nominee relationship should be disclosed to the company and to any relevant registry. Legal Practitioners must subject the UBOs behind nominee directors and shareholders to EDD per the FIA. They should further have measures to detect the possibility that undisclosed nominee arrangements may exist. Guidance Note 14 of 2023 avail some indicators of possible nominee arrangements. Policies, procedures and controls of the Legal Practitioner must ensure detecting undisclosed nominee arrangements will be identified and addressed as part of the CDD process and ongoing monitoring by the Legal Practitioner. The object is to request the nominee shareholder or director to avail identity of the UBO and subjecting both nominee and UBO to EDD measures as per sections 6.1 [(g) and 6.1.2] above. If nominee or relevant parties are evasive, give misleading information or do not cooperate, the Legal Practitioner should file a suspicious activity report with FIC as per section 33 of the FIA, without delay.

6.1.4 Bearer shares[16]

The Mutual Evaluation on Namibia[17] observed that *"the use of bearer shares is permitted in Namibia, however, no mechanisms have been implemented to guard against them being abused for ML or TF."* The risk emanating from bearer shares is further exacerbated by the lack of mechanisms to prevent the misuse of nominee shareholding and directorship.

[16] Simply put, bearer shares are negotiable instruments that accord ownership of a company to the person who possesses the share certificates, which are not registered and do not contain the name of the shareholder. Bearer shares permit ownership of the corporation to be transferred by simply handing over physical possession of the shares. Because ownership is never recorded in the share certificates, bearer shares are beyond the reach of the regulations and controls typically associated with registered shares.
[17] as per paragraph 405, page 120.

Legal Practitioners need to identify the use or involvement of bearer shares (especially when nominee arrangements exist) and ensure, to the extent possible, that the UBO can be subjected to EDD as the FIA. Sections 6.1(g) and 6.1.2 above avails EDD measures which ought to be undertaken. If the holders of bearer share certificates (or those in whose custody it is merely placed), nominees or relevant parties are evasive, give misleading information or do not cooperate, the Legal Practitioner should file a suspicious activity report with FIC as per section 33 of the FIA, without delay.

6.2 Ascertainment of information: Associations, NPOs, Partnerships etc.

Legal Practitioner must ascertain, in respect of an entity such as an association, a government organ/department, a representative office of a government, a non-governmental organisation, non-profit organization (NPO), an international organisation, an intergovernmental organisation as well as a legal person, or a foreign company or foreign close corporation -

a) the **registered name** of the entity, if so registered;
b) the **office or place of business**, if any, from which it operates;
c) the **registration number**, if any;
d) its **principal activities**; and
e) the **full name, residential address**, and one of the following, listed in the order of preference – the national identity number; the passport number; or date of birth, of the natural person purporting to be authorised (Part of Management or Director etc) to establish a business relationship or to enter into a transaction through the Legal Practitioner on behalf of such entity and each beneficial owner. Persons who **exercise such effective control** of a legal person or arrangement should be identified as per section 6.1(g), 6.1.2 and 6.1.3 above.

6.2.1 NPOs

It is generally accepted that Specified Non-Profit Organisations (NPOs) are highly vulnerable to TF. Not all NPOs are thus highly vulnerable. It is thus not risk based, nor required in law to subject

all NPOs to EDD. The 2020 NRA found Faith Based Organisations (FBOs) to be most vulnerable to TF domestically while the 2023 NRA update found NPOs involved in charitable activities as highly exposed to TF risks. This is in line with international trends and typologies. Legal Practitioners are therefore reminded that FBOs and charities, being Specified NPOs, generally present increased TF risks. Worth noting is that domestically, FBOs have also been greatly abused to advance ML activities. The Legal Practitioner shall, in addition to the CDD measures in 6.2 (and some elements in 6.1.2) above, ensure that FBOs and charities are subjected to the following:

a) conduct EDD of the customer (NPO and those acting on its behalf);
b) obtain **senior management's approval** while establishing business relationship but before availing any services;
c) gain assurance that the business relationship may **not be used for unlawful objects**;
d) issue any instructions, incorporation documents etc., **in the name of the relevant NGO, NPO or charity**, as given in its constituent documents and not other names;
e) subject the authorized agents or **representatives** of the customer to comprehensive CDD as stated herein (section 4.1.2 and 5 above); and
f) ensure that the NPO itself, its authorized agents or representatives are **not listed on any sanctions list nor affiliated directly or indirectly** with listed or proscribed persons or entities, whether under the same name or a different name.

6.2.2 Partnerships

Legal Practitioners must ascertain, in respect of a partnership, the following:

a) its name, or where applicable its registered name;
b) its office or place of business, if any, or, where applicable, its registered address;
c) where applicable, its registration number; and
d) the full name, residential address (if available), and one of the following, listed in the order of preference – the national identity number; the passport number; or date of birth, of each partner, including silent partners and partners *en commandite*, beneficial owners and any other natural person **who purports to be authorised** to establish a business relationship

or to enter into a transaction via the Legal Practitioner on behalf of the partnership. Persons who **exercise such effective control** of a partnership, legal person or arrangement should be identified as per section 6.1(g) (and some elements in 6.1.2) above. **Legal Practitioners must have measures to identify persons who could be 'directing or managing the affairs" of the partnership without appearing anywhere on any documents as partners or in some logically clear capacity. Beneficial owners or those controlling partnerships without being duly identified increase the ML/TF/PF risk exposure of partnerships.**

6.2.3 Trusts

A Legal Practitioner must ascertain the following in respect of a trust:

a) its **registered name**, if any;
b) the **registration number**, if any;
c) the **country where it was set up**, if the trust was set up in a country other than Namibia;
d) the **management company of the trust**, if any;
e) the **full name; the residential address, contact particulars and one of the particulars enumerated**, in the order of preference, under section 4.1.2 above, of each natural person who purports to be **authorised to establish a business relationship** or to enter into a transaction or transact with the Legal Practitioner on behalf of the trust; and
f) the **full name**, and one of the following, listed in the order of preference – national identity number; passport number; or date of birth; of the following persons –
   - ✓ each **trustee of the trust**;
   - ✓ each **beneficiary or class of beneficiaries** of the trust referred to by name in the trust deed or other founding instrument in terms of which the trust is created;
   - ✓ the **founder of the trust**;
   - ✓ each **person authorised to act on behalf of the trust**; and
   - ✓ each person **exercising ultimate effective control** over the trust or/and each beneficial owner.

g) If the beneficiaries of the trust are not referred to by name in the trust deed or founding instrument in terms of which the trust is created, the Legal Practitioner must follow the natural person identification procedure stated herein above [section 6.1(g) and some elements of 6.1.2] to ascertain the names of the beneficiaries and document the method of determining such beneficiaries. **Legal Practitioners must have measures to identify persons who could be 'directing or managing the affairs' of the trust without appearing anywhere on any documents as trustees or other beneficial owner or in some logically clear capacity. Beneficial owners or those controlling trusts without being duly identified increase the ML/TF/PF risk exposure of partnerships. The information below helps identify various types of UBOs in trusts.**

6.2.3.1 Risks 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*[18] may have been abused in advancing ML. All such trusts were all (100%) Namibian initiated or founded (owned). Also, none of them 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. For risk mitigation purposes, *inter-vivos* trusts are high risk. With beneficial owners in trusts, Namibian and South African citizens present the highest risks.

6.2.3.2 Trust Founder[19]

a) A founder is generally any **person (or persons) by whom the trust was made**. A person is a founder if he or she has provided (or has undertaken to provide) property or funds directly or indirectly for the trust. This requires there to be an element of bounty (i.e. the founder must be intending to provide some form of benefit rather than being an independent third party transferring something to the trust for full consideration);

[18] Trusts created between living persons registered under the Trust Moneys Protection Act 34 of 1934.
[19] Trust Founder or the person who establishes the trust. Sometimes referred to as the Settlor in other jurisdictions.

b) A founder **may or may not be named in the trust deed**. To combat ML/TF/PF risks as per the FIA, Legal Practitioners should have policies and procedures in place to identify and verify the identity of the real economic founder;

c) A **Legal Practitioner establishing on behalf of a client or administering** a trust, company or other legal entity or otherwise acting as or providing a trustee or director of a trustee, company or other legal entity should have policies and procedures in place (taking a risk based approach) to **identify the source of funds** in the trust, company or other legal entity;

d) When need be, **obtain supporting information** that may help establish source of funds. It may be more difficult (if not impossible) for older trusts to identify the source of funds, where contemporaneous evidence may no longer be available. Evidence of source of funds may include reliable independent source documents, data or information, share transfer forms, bank statements, deeds of gift, letter of wishes etc.; and

e) Where assets have been **transferred to the trust from another trust,** it will be necessary to **obtain this information for both transferee and transferor** trust.

6.2.3.3 Identifying natural persons exercising effective control

Identifying the natural persons exercising effective control of trusts is essential in the UBO related due diligence. The below is essential in such efforts:

a. A Legal Practitioner providing services to the trust should have **procedures in place to identify any natural person** exercising effective control over the trust;
b. For these purposes "control" means a power (whether exercisable alone or jointly with another person or with the consent of another person) under the trust instrument or by law to:

i. dispose of or invest (other than as an investment manager or adviser) trust property;
ii. direct, make or approve trust distributions;
iii. vary or terminate the trust;
iv. add or remove a person as a beneficiary or to or from a class of beneficiaries and/or; and
v. appoint or remove trustees.

c. Legal Practitioner who administer the trust or otherwise act as trustee must, in addition, also obtain information to satisfy itself that it knows the **identity of any other individual who has power to give another individual** "control" over the trust; by conferring on such individual powers as described in paragraph (b) above;

d. In certain cases, the founder, beneficiary, protector or other person exercising effective control over the trust may be a company or other legal entity. In such a case, the Legal Practitioner should have policies and procedures in place to enable it to identify (where appropriate) the beneficial owner or controlling person in relation to that entity.

6.2.4 Identifying beneficiaries

a. In the case of a **beneficiary which is an entity** (e.g a charitable trust or company), the Legal Practitioner should satisfy itself that it understands the reason behind the use of an entity as a beneficiary. If there is an individual beneficial owner of the entity, the Legal Practitioner should satisfy itself that it has sufficient information to identify the individual beneficial owner;

b. Where the **beneficiaries of the trust have no fixed rights to capital and income** (e.g discretionary beneficiaries), a Legal Practitioner should obtain information to enable it to identify the named discretionary beneficiaries (e.g. as identified in the trust deed);

c. Where **beneficiaries are identified by reference to a class** (e.g. children and issue of a person) or where beneficiaries are **minors under the law governing the trust**, although a Legal Practitioner should satisfy itself that these are the intended beneficiaries (e.g. by reference to the trust deed), the Legal Practitioner is not obliged to obtain additional information to verify the identity of the individual beneficiaries referred to in the class unless or until the trustees determine to make a distribution to such beneficiary;

d. In some trusts, named individuals only become beneficiaries on the happening of a particular **contingency** (e.g. on attaining a specific age or on the death of another beneficiary or the termination of the trust period). In this case, Legal Practitioners are not required to obtain additional information to verify the identity of such contingent beneficiaries unless or until the contingency is satisfied or until the trustees decide to make a distribution to such a beneficiary; and

e. Legal Practitioners who administer the trust or company or other legal entity owned by a trust or otherwise provide or **act as trustee or director to the trustee**, company or other legal entity should have procedures in place so that there is a requirement to **update the information provided if named beneficiaries are added or removed** from the class of beneficiaries, or beneficiaries receive distributions or benefits for the first time after the information has been provided, or there are other changes to the class of beneficiaries.

6.2.4.1 Identifying Individual and Corporate trustees

a. Where a **Legal Practitioner is not itself acting as trustee**, it is necessary for the Legal Practitioner to obtain information to enable it to identify and verify the identity of the trustee(s) and, where the trustee is a corporate trustee, identify the corporate, obtain information on the identity of the beneficial owners of the trustee, and take reasonable measures to verify their identity;

b. Where the **trustee is a listed entity (or an entity forming part of a listed group) or an entity established and regulated** to carry on trust business in a jurisdiction identified by

credible sources **as having appropriate AML/CFT/CPF laws, regulations and other measures**, the Legal Practitioner should obtain information to enable it to satisfy itself as to the identity of the directors or other controlling persons. A Legal Practitioner can rely on external evidence, such as information in the public domain, to satisfy itself as to the beneficial owner of the regulated trustee (e.g the website of the body which regulates the trustee and of the regulated trustee itself); and

c. It is not uncommon for families to set up **trust companies** to act for trusts for the benefit of that family. These are sometimes called private trust companies and may have a restricted trust licence which enables them to act as trustee for a limited class of trusts. Such private trust companies are often ultimately owned by a fully regulated trust company as trustee of another trust. In such a case, the Legal Practitioner should satisfy itself that it understands how the private trust company operates and the identity of the directors of the private trust company and, where relevant, the owner of the private trust company. Where the private trust company is itself owned by a listed or regulated entity as described above, the Legal Practitioner does not need to obtain detailed information to identify the directors or controlling persons of that entity which acts as shareholder of the private trust company.

7. EXTENT OF EDD

The EDD measures explained herein are extensive but not comprehensive. The extent to which a Legal Practitioner may go in carrying out EDD cannot be fully prescribed. Circumstances of each scenario should ideally dictate the nature and extent of relevant EDD measures. Generally, Legal Practitioners are not obliged to obtain other information about UBOs other than to enable the Legal Practitioner to satisfy itself that it knows who the UBOs are or identify whether any named beneficiary or beneficiary who has received a distribution from a trust/legal entity is a high risk client (e.g PEP, sanctioned person etc.).

8. SUSPICIOUS TRANSACTION OR ACTIVITY REPORTS (“STRs/SARs”)

The primary reason for due diligence and monitoring transactions carried out by clients is to ensure that such transactions are consistent with the Legal Practitioner’s knowledge of the client, the

client's commercial or personal activities and risk profile. Suspicions are often detected from client behaviour or activities outside the known client profile. Thus, understanding client profile is essential as it places the Legal Practitioner in positions to effectively detect and report suspicions when they arise. Guidance Note 14 of 2023 helps detail high risk situations, clients and activities that may be suspicious.

New report types have been introduced to enhance effectiveness. With effect from 17 April 2023, TF and PF suspicions, as well as sanctions screening name matches shall no longer be reported through STRs and SARs on goAML. TF and PF suspicions shall only be reported through TPFA and TPFT reports, as explained in section 8 herein below. Similarly, sanctions screening name matches shall only be reported through Sanctions Name Match Activity reports (SNMAs). Only ML suspicions shall be reported through STRs and SARs..

STRs are reports that explain **suspicious transactions** for ML. The term suspicion is meant to be applied in its everyday, normal sense. The suspicion, as an example, could be the funds involved in the transaction are the proceeds of any crime or linked to terrorist activity. The Legal Practitioner does not need to know what sort of crime may have been committed, but one or more red flags or warning signs of potential ML, which cannot be reasonably explained by the customer, should be adequate to reach the standard of what constitutes a suspicion worth reporting to the FIC.

SARs are reports which, under normal circumstances explain potential **suspicious activity** related to clients but may not necessarily be transactions whereas STRs refer to actual suspicious transactions. For example, if a client attempts to transact and after EDD enquiries does not proceed with finalizing the transaction, and the activities or his/her behaviour around such is suspicious, then the appropriate report to file with the FIC is a SAR and not a STR (because no transaction occurred).

8.1 Practical controls

Operating frameworks or controls in the Legal Practitioner must enable the following:

a) Staff must raise an internal report where they know or suspect, or where there are reasonable grounds for having knowledge or suspicion that persons involved in the transaction could be engaged in ML, TF or PF;
b) The Legal Practitioner's AML Compliance Officer, or their appointed alternative, must consider all such internal reports. The Compliance Officer must submit the relevant report to the FIC via GoAML;
c) Such relevant report should be reported **without delay** (within a few hours of detecting the suspicion) to enhance the effectiveness of combatting activities;
d) After filing such report, the Legal Practitioner should consider all risk exposure and whether it is prudent to continue availing services to such client;
e) It is a criminal offence for anyone, following a disclosure to a Compliance Officer or to the FIC, to do or say anything that might either 'tip off' another person that a disclosure has been made or prejudice an investigation. A Legal Practitioner's policies should clearly state this;
f) Important actions required:
   - ✓ enquiries made in respect of internal reports (red flags) must be recorded;
   - ✓ the reasons why a report was, or was not submitted should be recorded;
   - ✓ keep a record of any communications to or from the FIC about a suspicious transaction or activity report.

The requirement to report to the FIC should be supported by the following (within the Legal Practitioner's AML/CFT Procedures):

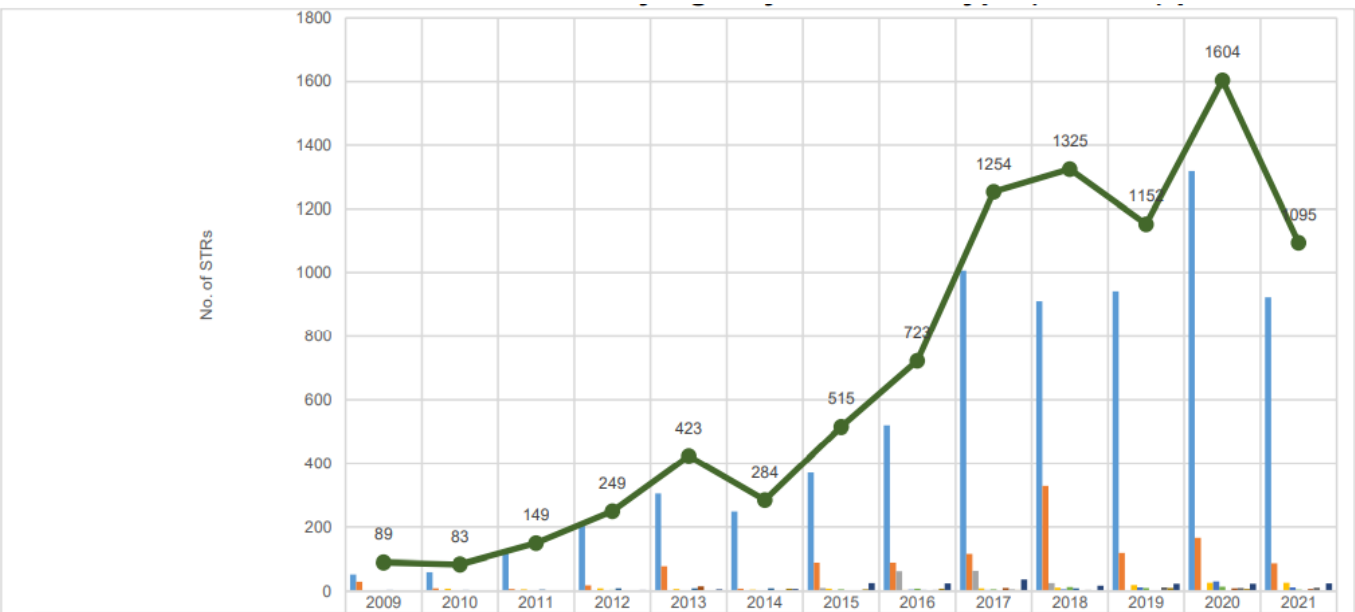
g) Staff internal reporting line to the AML Compliance Officer;
h) Confidentiality of reports, i.e. how to deal with customers, and others involved in a transaction, after an internal or external report has been made.

8.2 Sectoral Reporting Behaviour

The Mutual Evaluation on Namibia[20] found that STR and SAR reporting is not aligned to the country's risk exposure as banks tend to be the only sector detecting and reporting as per their risk exposure. This is an observation we have always known as a country. Overall, 8,945 STRs were received by the FIC since the reporting obligation commenced until 31 December 2021 (see Chart below). The banking sector submitted the most reports in such period, filing 78% (or 6,991) of reports followed by ADLAs[21] who submitted 13% (or 1,140). The high number of reports from the banking sector could be attributed to various factors, including the fact that banks appear to have the most matured AML/CFT/CPF control systems (enhanced ability to detect and report). It can also be argued that banking services are inherently exposed to a higher risk of abuse as almost all other sectors make use of the banking systems. For Legal Practitioners however, the reported volumes of STRs are deemed inadequate, given the sector's risk level. The sector's reporting volumes could be enhanced.

[20] Adopted in September 2022: Report available at: https://www.esaamlg.org/reports/MER%20of%20Namibia-September%202022.pdf

[21] Authorised Dealers in Foreign Currency with Limited Authorization often known as Bureaus de Changes.

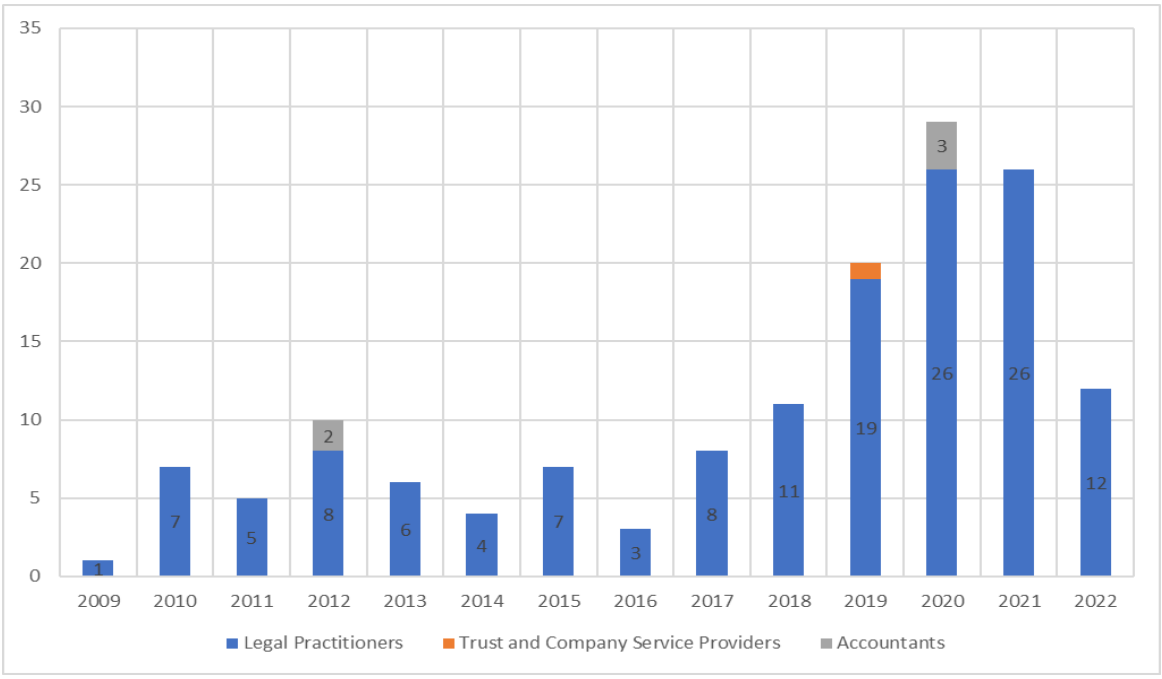


	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Banks	52	59	129	206	305	248	371	519	1007	911	942	1319	923
ADLAs	29	9	6	18	78	7	89	89	115	329	118	166	87
Insurance/Investment Brokers	2	0	0	1	0	0	10	62	63	25	2	0	0
Legal Practitioners	1	7	5	8	6	4	7	3	8	11	19	26	26
Asset Management Companies	0	1	2	1	2	1	0	4	3	5	12	30	12
Motor Vehicle Dealers	0	1	0	3	2	1	5	7	5	13	10	14	4
Financial Intelligence Units	3	3	1	0	0	8	1	3	0	8	2	2	1
Long Term Insurance Companies	0	0	1	0	15	2	0	2	10	2	2	8	6
Unit Trust Schemes	1	1	1	0	0	0	2	3	4	3	12	10	11
Individual Persons	0	0	0	0	1	7	5	7	3	1	10	6	1
Others	1	2	1	3	5	6	25	24	36	17	23	23	24
Total	89	83	149	249	423	284	515	723	1254	1325	1152	1604	1095

Classification of STRs as received from various sectors

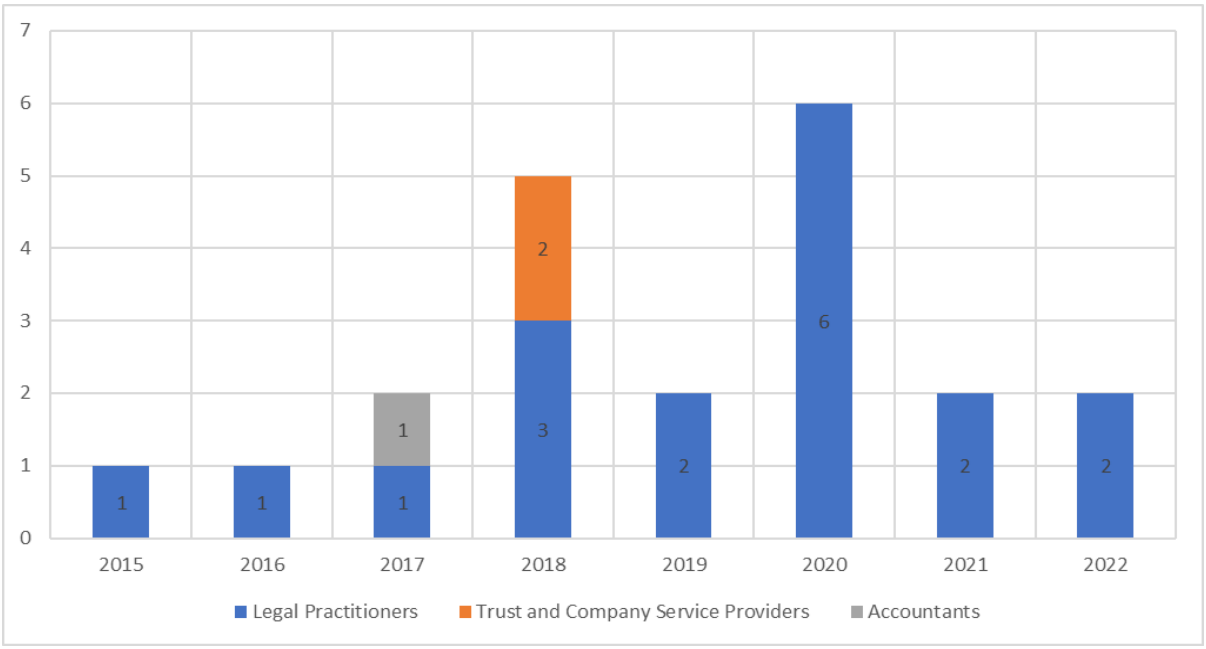
8.2.1 Legal Practitioners STR Reporting

While the FIC findings from compliance assessments suggests Legal Practitioners can do more, the table below suggests Legal Practitioners are the highest reporting sub-sector within sectors reporting similar services.



8.2.2 Legal Practitioners SAR Reporting

Similar to STRs, the table below suggests Legal Practitioners are the highest reporting sub-sector amongst other sectors availing similar services.



9. RECORD KEEPING

9.1 What Records must be kept?

a. the identity, address and all such client identification records as stated in parts 4 - 6 herein;
b. the date, time and involved financial amounts of client's activities/transactions;
c. information relating to all relevant reports escalated to the FIC; and
d. any other information which the FIC may specify in writing.

Legal Practitioners should satisfy themselves that the records they obtain would meet the required standard as per the FIA and summarised herein.

9.2 Who must keep records?

The Legal Practitioner (as Accountable Institution) ought to keep records as per the FIA. A third party may keep records on behalf of a Legal Practitioner but the Agent remains ultimately accountable for ensuring such records are kept as per the FIA. Legal Practitioner must engage the FIC when proposing to outsource record keeping responsibilities as per the FIA. Further, the records of two or more Accountable or Reporting Institutions that are supervised by the same supervisory body can be centralised.

9.3 Manner of Record Keeping

The records must be kept:

a. in a manner that protects the integrity of the transaction;
b. in a manner which permits reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity or civil asset forfeiture procedures. The Golden Rule with record keeping is enabling an effective reconstruction of identification or transacting activities by competent authorities.

Further, records can be kept in hard copy or electronic format as long as a paper copy can be readily produced, especially for law enforcement purposes. Legal Practitioner should maintain effective record-keeping systems to enable the FIC and other relevant authorities to access such records in a timely fashion.

9.4 Period for which records must be kept

Records that relate to the establishment of a business relationship (e.g client identification records) must be kept as long as the business relationship exists and for at least five years from the date on which the business relationship is terminated. Records that relate to single transactions must be kept for five years from the date on which the transaction was concluded. Records that relate to copies of reports submitted to the FIC must be kept for a period of not less than five years from date of filing such report. However, records must be kept for longer than the 5-year period if the Legal Practitioner is requested to do so by the FIC, the Office of the Prosecutor-General or by any other law enforcement body.

10. UNSC SANCTIONS SCREENING

The object of sanctions screening is to implement Targeted Financial Sanctions (TFS) towards anyone listed by the UNSC.

Legal Practitioners are expected in terms of section 24 and Regulation 15(5)[22] of the FIA to screen clients or potential clients involved in transactions against the relevant sanctions lists issued by the United Nations Security Council (UNSC). Such screening should take place before accounts are opened or client is granted access to services, regardless of whether the client transacts below or above the CDD threshold. If the Legal Practitioner in any way makes use of middlemen or

[22] Accountable institution to conduct on-going and enhanced customer due diligence: (5) An accountable institution must also, in the process of monitoring, screen - (a) names of prospective clients, before acceptance of such a client; (b) names of existing clients, during the course of the business relationship; and (c) all the names involved in any transaction, against the sanctions lists issued by the United Nations Security Council under Chapter VII of the United Nations Charter for purposes of combating the financing of terrorism and the funding of proliferation activities.

brokers/agents to facilitate or avail services, the Legal Practitioner needs to ensure that such third parties duly attend to their AML/CFT/CPF responsibilities if any reliance is placed on them. This is essential to combat TF and PF activities by ensuring designated persons, organizations or countries are identified and not unduly availed services, while their assets and funds are accordingly frozen. The term Targeted Financial Sanctions primarily speaks to **asset freezing without delay** and **prohibition** from making funds or other assets or services, directly or indirectly, available for the benefit of sanctioned individuals, entities, or groups.

Locally, the National Security Commission (NSC) is the body with statutory responsibilities in terms of the PACOTPAA[23] to propose persons or entities to the 1267/1989 Committee for designation and for proposing persons or entities to the 1988 Committee for designation. To date, the NSC has not seen the need to designate any person. Legal Practitioners are required to continue screening against relevant sanctions lists as explained above.

Screening against other designations lists such as OFAC, though not mandatorily required by domestic laws is very helpful in the overall risk management effectiveness. For any transactions or currency exchanges in USD for example, there is an inherent requirement to screen involved parties against the OFAC list. Similarly, when dealing in British Pounds or the Euro, screening against lists issued by such relevant authorities is an inherent requirement.

This section avails basic guidance on TFS. Legal Practitioners are required to further consider the detailed guidance around reporting, sanctions screening and TFS contained in Guidance Note 07 of 2023.

10.1 Effective Client Screening

In order to effectively implement Targeted Financial Sanctions (TFS), Legal Practitioners must ensure:

[23] Prevention and Combating of Terrorist and Proliferation Activities Act, 2014 (Act No. 4 of 2014).

a. sanction screening is performed on all clients before availing them services; and

b. no services are availed to clients before the sanction screening is completed and evidence of same has been documented. Screening should **not be undertaken after** availing services or facilitating transactions. Prior screening **enables proactive detection of sanctioned persons.** If such sanctioned persons are detected, such should not be granted access to any services at all and their attempted transactions should be reported to the FIC promptly and without delay, while the assets (or funds) involved are frozen or further transactions prohibited, as per the FIA and PACOTPAA. **In practice, policies and operating procedures therefore need to ensure clients are allowed to at least attempt the transaction to ensure due identification, which will enable effective screening and, if client is listed, eventual freezing of the funds which the client attempted to transact with, followed by complete prohibition to transact any further and reporting.**

The following databases of the Legal Practitioner must be included in the screening process:

a. Existing customer databases. All systems (if any) containing customer data and transactions need to be mapped to the screening system to ensure full compliance;
b. Potential customers before conducting any transactions or entering a business relationship with any person;
c. Names of parties to any transactions (e.g., buyer and seller of legal persons; any party or beneficial owner of an entity or trust to be registered etc.[24]);
d. Ultimate beneficial owners, both natural and legal;
e. Names of individuals, entities, or groups with direct or indirect relationships with them; and
f. Directors and/or agents acting on behalf of customers (including individuals with power of attorney).

[24] Other sectors such as Banks need to include agents, freight forwarders, vessels etc.

10.2 Where to find the updated Sanctions Lists?

As mentioned above, Legal Practitioners, like all other Accountable and Reporting Institutions are required to access lists of sanctioned persons and screen their clients against such lists before establishing a business relationship and whenever the sanctions lists is updated. Domestically, at the time of issuing this Guidance, the NSC has not designated or listed any persons yet. At an international level however, the information on designated individuals, entities or groups in the Sanctions Lists is subject to change. The most recently updated sanctions list of the UNSC[25] can be found on the UNSC website or via the following link: https://www.un.org/securitycouncil/content/un-sc-consolidated-list

10.3 Targeted Financial Sanctions (TFS)

As mentioned above, TFS includes **asset freezing without delay** and **prohibition** from making funds or other assets or services, directly or indirectly, available for the benefit of sanctioned individuals, entities, or groups.

10.3.1 Asset freezing without delay

In terms of international standards, without delay means **within a matter of hours**. Freezing is the prohibition to transfer, convert, dispose, or move any funds or other assets that are owned or controlled by designated individuals, entities, or groups in the Local Terrorist List or UN Consolidated List. It includes:

a. The freezing of funds and other financial assets and economic resources, and includes preventing their use, alteration, movement, transfer, or access; and
b. The freezing of economic resources also includes preventing their use to obtain funds or other assets or services in any way, including, but not limited to, by selling or mortgaging them.

[25] The UNSC has a UN Consolidated List of all the sanctioned individuals, entities, or groups designated by the United Nations Sanctions Committees or directly by the UNSC.

Examples of freezing:

i. ***Financial Institutions:*** *a freezing measure can be suspending listed client's access to bank accounts which have funds or blocking transactions which can deplete such;*

ii. ***DNFBPs like Accountants and law firms:*** *a freezing measure can be holding onto any funds, assets the client may have deposited with the Accountant/Law Firm (including payment for services) while discontinuing the client's requested services or transactions. Could be blocking the transfer of ownership of legal entities, stopping the registration of such as requested by client.*

10.3.2 Prohibition

The principle is prohibition from making funds or other assets or services available. This means the prohibition to provide funds or other assets to or render financial or other services to, any designated individual, entity, or group.

Examples of prohibition:

i. ***Financial institutions:*** *prohibition from offering banking or transactional services;*

ii. ***DNFBPs, like Accountants and law firms:*** *prohibiting the provision of any services, such as agency or legal services to transfer entity ownership, buying or selling entity, shares etc.*

10.3.3 Object of freezing and prohibition

Note however that even when freezing measures are taken or enacted, there should be no restrictions on client introducing or depositing more funds with the Legal Practitioner (e.g paying further funds towards services or as part of entity/shares acquisition etc). As long as the service which the listed client so desires cannot be finalised for them, prohibition and asset freezing requirements will be met on condition whatever has already been frozen is not further depleted. The object remains to deprive listed/designated/proscribed persons from as much funds/assets as possible so they can be denied access to resources which may be used to fund terrorist or

proliferation activities. This is the essence or primary goal of TFS measures. Legal Practitioners need to consider appropriate implementation given the circumstances they may find themselves in, with each transaction/client.

10.4 Reporting Possible Matches

The mechanism to report any freezing or suspension measures taken upon identifying confirmed or potential matches is through the goAML platform. The use of the goAML platform for TFS reporting purposes eases the burden of reporting and avails the necessary confidentiality required for this sensitive process. As mentioned above, institutions should no longer report sanctions screening matches, TF or PF suspicions via STRs or SARs. New report types have been created to enhance effectiveness, especially around TFS measures. From 17 April 2023, sanctions screening matches as well as TF and PF suspicions or transactions should be reported as per below:

Reportable Activity or Transaction	Type of Report
Detection of a possible **sanctions screening match.**	SNMA - Sanction Name Match Activity report
Reporting any other **Activity** (or attempted transaction which was not completed) which may point to, or be linked to potential terrorism, TF or PF.	TPFA - Terrorist & Proliferation Financing Activity report
Reporting any other **Transaction** (actual transacting) which may point to, or be linked to potential terrorism, TF or PF.	TPFT- Terrorist & Proliferation Financing Transaction report

The following information must be shared when submitting a SNMA report:

a. The full name of the ‘confirmed match’. Attach ID documents of the ‘confirmed match’, such as passport or other ID documents for individuals, and relevant legal person incorporation documents such as CC incorporation forms, articles of association, trust establishing documents etc.; and
b. Amount of funds or other assets frozen (e.g., value of real estate, value of funds in bank accounts, value of transactions, value of securities, etc.). Attach proof documents such

as bank statements, transaction receipts, securities portfolio summary, title deeds, etc., if such are at hand.

When a possible match is reported to the FIC, the FIC or such relevant competent authorities will direct all activities related to the frozen assets or funds. The Legal Practitioner may not release frozen assets or do anything related to such assets without being instructed to do so.

11. ROLE OF AML COMPLIANCE OFFICER

The effectiveness of the Compliance Officer[26] usually impacts an Accountable Institution's overall risk management level. The AML/CFT/CPF controls within a Legal Practitioner should therefore ensure the Compliance Officer is placed in a position to execute his/her FIA responsibilities as required. Such responsibilities primarily include ensuring that:

a. internal ML/TF/PF risk assessments are undertaken and results thereof duly implemented. Periodically, such risk assessments are duly revised or updated in line with SRAs, NRAs, typology reports locally and internationally;
b. the AML/CFT/CPF Controls (policies, procedures etc) are at all times aligned to risk levels;
c. front-line staff (staff members who directly deal with customers) are duly trained on CDD measures as per the FIA;
d. he/she undertakes monitoring transactions, e.g. routine or spot checks based on risks;
e. measures to internally detect and escalate[27] potential ML/TF/PF indicators or red flags are prudent and enable the required level of confidentiality;
f. he/she files relevant reports to the FIC, without delay;
g. he/she regularly reports to senior management about AML/CFT performance; and
h. he/she attends to any other activities necessary to enhance FIA compliance.

Compliance Officers ought to have adequate managerial authority and capacity within an Accountable Institution to lead compliance activities, as per the FIA. With one-man Legal

[26] Appointed as per Section 39 of the FIA.
[27] To the Compliance Officer for analysis and decision on whether to report same to the FIC.

Practitioners, Accountants or Law Firms, the individual has a responsibility to attend to all the responsibilities of a Compliance Officer duly. Depending on the size of the Legal Practitioner, volume of transactions, overall risk etc., regard has to be had with the Legal Practitioner's ability to duly attend to all responsibilities as per the FIA. Such factors should guide resourcing of a Compliance function.

12. GENERAL

This Guidance 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 herein is intended to only provide a summary on these matters and is not intended to be comprehensive.

13. NON-COMPLIANCE WITH THIS GUIDANCE

This document is a guide. Effective implementation is the sole responsibility of Accountable and Reporting 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 satisfaction of the FIC as the supervisory body.

14. GENERAL

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