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. 08 OF 2023

GUIDANCE ON RISK ASSESSMENTS AND ML/TF/PF INDICATORS: DEALERS IN PRECIOUS METALS AND STONES

First Issued: 12 June 2023

TABLE OF CONTENTS

DEFINITIONS AND ABBREVIATIONS

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

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

“CDD” means Customer Due Diligence;

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

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

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

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

“DPMS” means Dealers in Precious Metals and Stones. These are persons who carry on the business of trading in minerals specified in Schedule 1 of the Minerals (Prospecting and Mining) Act, 1992 (Act No. 33 of 1992;

"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;

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

“TF” means Terrorist Financing;

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

1. BACKGROUND

This document avails sectoral guidance on conducting risk assessments and indicators of common Money Laundering (ML), Terrorism and Proliferation Financing (TF/PF) activities. It contains Guidance on how designated Dealers in Precious Metals and Stones (DPMS) should conduct ML/TF/PF risk assessments, as part of their compliance obligations. Risk assessment outcomes highlight risk levels and point to areas that may need prioritization in control implementation. Guidance Note 09 of 2023, issued along with this Guidance Note, provides essential guidance on how DPMS effectively implement mitigating controls as per risks identified.

This Guidance Note is issued in terms of Section 9(1)(h) of the Financial Intelligence Act, 2012 (The FIA). It is the first of two sectoral guidance notes for all DPMS who carry on the business of trading in minerals specified in Schedule 1 of the Minerals (Prospecting and Mining) Act, 1992 (Act No. 33 of 1992). Importantly, they are only required to implement FIA controls when they engage in transactions wherein their customers and/or counterparties make payments in cash amount to NAD 5,000.00 or more. This naturally means no FIA obligations arise for the sector for all non-cash transactions (e.g electronic transfers).

The Financial Intelligence Centre (FIC) issues this Guidance to help DPMS implement and enhance their internal Anti-Money Laundering, Combatting the Financing of Terrorism and Proliferation (AML/CFT/CPF) measures. It is common cause that services offered by DPMS have been abused for ML domestically, as reflected through cases prosecuted. The 2020 NRA documents statistics of cases investigated and prosecuted involving precious stones and metals. Internationally, there are trends and typologies which suggest such abuse to advance TF/PF activities. The characteristics of precious metals and stones which make them attractive to money launderers are equally attractive to those advancing TF and PF.

A risk assessment is familiar to dealers in diamonds, jewels and precious metals because of the risks of theft and fraud which they naturally want to mitigate. The primary objective of this guidance is to help the sector add ML/TF/PF risks to those traditional industry

concerns (theft and fraud), in a more formal structured program. Risk assessment and management would not be new to diamond dealers in particular given their familiarity to same owing to the worldwide Kimberley Process[1] which is designed to ameliorate risks of conflict finance in rough diamonds.

2. SOURCES OF INFORMATION

This Guidance relied on information from FIC's FIA Compliance Assessments, various national and sectoral risk assessments conducted over the years, the FATF Guidance for a Risk Based Approach for DPMS[2], FATF and Egmont[3] study, ESAAMLG study[4] in illicit Dealings in Gold, Diamond, Rubies and Associated Money Laundering and Terrorist Financing in the ESAAMLG Region, on amongst others.

3. COMMENCEMENT

This Guidance Note comes into effect on **12 June 2023**.

4. SCOPE OF DPMS

4.1 Cash Transactions Above Threshold

The FIA is informed by international instruments which lay the foundation for how Namibia and all other countries should contribute to international ML/TF/PF risk management in

[1] A worldwide regulatory scheme that governs the movement of rough diamonds across international borders, adding a certificate of the legitimacy of the trade of the diamonds and a statement of value to all rough diamonds traded across borders. It is supplemented by dealer warranties applicable to polished diamonds and jewelry containing diamonds covering each trade down to retail sales. The Kimberley Process includes all significant dealers and countries involved in diamond mining, trading and processing, and its tracking and valuation system.

[2] FATF Guidance on RBA for Dealers in Precious Metals and Stones, June 2008. Accessed via: file:///C:/Users/ham638/Downloads/RBA%20for%20Dealers%20in%20Precious%20Metal%20and%20Stones%20(2).pdf

[3] FATF and Egmont Study on ML and TF Through Trade in Diamonds, October 2013. Accessed via: https://egmontgroup.org/wp-rcontent/uploads/2021/09/2013_ML_TF_through_Trade_in_Diamonds_and_Precious_Stones_%E2%80%93_Joint_EG_and_FATF_Report_.pdf

[4] ESAAMLG Study in illicit Dealings in Gold, Diamond, Rubies and Associated Money Laundering and Terrorist Financing in the ESAAMLG Region, March 2022. Accessed at: https://www.esaamlg.org/reports/ILLICIT_DEALING_SEPT_2022.pdf

safeguarding our financial system. The FATF Recommendations inform the provisions of the FIA.

The FATF Recommendations isolate the responsibility of DPMS only to high risk circumstances. Recommendation 22 in particular provides that the compliance obligations to this sector only arise when:

a. the DPMS engages in any **cash transactions**; and
b. such cash transaction is equal to or **above the prescribed CDD threshold**.

At the time of issuing this guidance, such threshold in Namibia is still NAD 5,000.00. It means, a DPMS only becomes an Accountable Institution with compliance obligations when participating in a cash transaction above such threshold. At the time of this publication, this threshold is being revised and indications are that it will be increased. Publications will be issued after finalisation of same.

Keep in mind the need to identify related multiple cash transactions in excess of such threshold as criminals can structure transactions below such due diligence thresholds. This may be rare given the higher amounts traded in the industry. At the time of issuing this document, national efforts are at an advanced stage to revise and possibly increase such threshold.

4.1.1 Reasons for Cash Transactions and Threshold

The FATF advocates for a Risk Based Approach in mitigating risks. This is premised on identifying priority areas and focusing on such. The FATF Study (2013) earlier cited indicates the following as factors which informed the decision to limit the said due diligence requirements to cash transactions for DPMS:

a. there is an informal knowledge of the actual and potential customers due to the recurring business activities and transactions conducted; or
b. these requirements are covered by other reporting and registry obligations, mainly related to prudential regulation, taxes or accounting.

While this is true for Business-to-Business transactions, the situation is different with retail transactions or sales directly to the customer. The said FATF study5 equally observed that the extent of cash usage is generally diminishing and that most of the transactions are not conducted in cash.

4.1.2 Relative Exclusions

Despite the above FATF Recommendation 32 on Cash couriers and its interpretative note should be duly considered. Such provide that precious metals and stones are not included in the scope of cash couriers, despite their high liquidity and use in certain situations as a means of exchange or storing and transmitting value. Their inclusion in the list of cash couriers may be from a Customs regulatory point of view.

While there is no obligation for FIA compliance when a transaction's payment method is via wire transfers or other means of electronic payment, note that digital movements of values such as cryptocurrencies or assets are not explicitly excluded. These digital platforms have greater anonymity which is the opposite of conventional payments in the common financial systems.

4.2 Understanding Precious Metals and Stones

In keeping with international AML/CFT/CPF frameworks on this subject, the context within which precious metals, stones6 and jewellery are defined is as follows:

a. *"Precious metal"* means:
   - Gold, silver, platinum, palladium, osmium, rhodium, iridium and ruthenium; and
   - includes any object which is composed of gold, silver, platinum or palladium etc.;
b. "*Precious stone*" includes, but not limited to diamonds, emeralds, rubies and sapphires;

[5] FATF and Egmont Study, Oct 2013.
[6] Minerals (Prospecting and Mining) Act 33 of 1992.

c. "*Semi-precious stones group*" includes, but not limited to Amazonite, aventurine, beryl, chrysoberyl, chrysocolla, cordierite, dioptase, dumortierite, garnet, milarite, quartz, sodalite, topaz, tourmaline and turquoise; and
d. "*Jewellery*" means any article made of a precious metal, stone or it allow, and which carries significant value (in this context it is determined in terms of CDD thresholds).

4.3 Inclusion in the Scope of DPMS

As mentioned herein above, a person or institution becomes a DPMS with FIA compliance obligations when carrying on the business of trading in minerals specified in Schedule 1 of the Minerals (Prospecting and Mining) Act, 1992 (Act No. 33 of 1992). Institutions listed in Schedule 1 of the FIA are Accountable Institutions (AIs) and are inherently exposed to higher ML/TF/PF risks, unless risk levels are determined to be low. AIs are thus required to comply with all the primary preventative AML/CFT/CPF obligations as per the FIA.

For purposes of this guidance, the term "dealer" encompasses a wide range of persons engaged in the precious stones and metals value chain, including:

a. those who produce precious metals or precious stones at mining operations;
b. intermediate buyers and brokers;
c. importers and exporters of precious stones and metals;
d. processing, refining or carrying out any value adding work on precious stones and metals in different ways. Includes precious stone cutting, polishing, refining and melting with the aim of adding value or transporting same;
e. jewellery manufacturers who use precious metals and precious stones;
f. those who retail precious stones and metals to the public; and
g. buyers and sellers in the secondary and scrap markets.

The focus is on any person carrying out the stated activities and not whether they identify themselves as a DPMS because DPMS can take different forms as listed above.

4.4 Exclusion from Definition of DPMS

FATF Recommendation 28 requires that DPMS be subject to effective systems for monitoring and ensuring compliance with AML/CFT requirements, which should be performed on a risk-sensitive basis by a supervisor or by an appropriate self-regulatory body. The selective recognition of some sectors as Accountable or Reporting Institutions and application of compliance obligations to specified transactions speaks to the risk based approach (risk sensitive) object of the FATF.

It is common cause that Reporting Institutions (RIs), unlike AIs, are generally exposed to lower ML/TF/PF risks. Dealers in Jewellery, Antiques and Arts are all listed in Item 4 of Schedule 3 of the FIA as RIs. This Guidance Note applies to Dealers in Jewellery but does not apply to Dealers in Antiques and Arts. DPMS, as cited herein thus includes Dealers in Jewellery. The Cabinet Approved 2020 National Risk Assessment (NRA) found that Dealers in Jewellery, Arts and Antiques' along with some other sectors are exposed to Very Low ML/TF/PF risks, confirming the rationale for maintaining such sectors as RIs in the FIA. RIs are thus expected to comply with minimal FIA obligations. Directive 02 of 2023 simplifies such obligations. The proposed FIA amendments, which are at Parliament at the time of issuing this guidance will further isolate and crystalise such minimal compliance obligations applicable to RIs.

5. STAGES OF ML IN DPMS

There are different methods employed to advance ML but the main stages thereof remain the same. The following are generally the main stages of ML:

A. Placement

Involves placing the proceeds of crime in the financial system. *For example, buying precious metals with proceeds of crime and later selling such with funds being paid into*

a bank account - with bank having limited means of establishing the illicit origin of such proceeds.

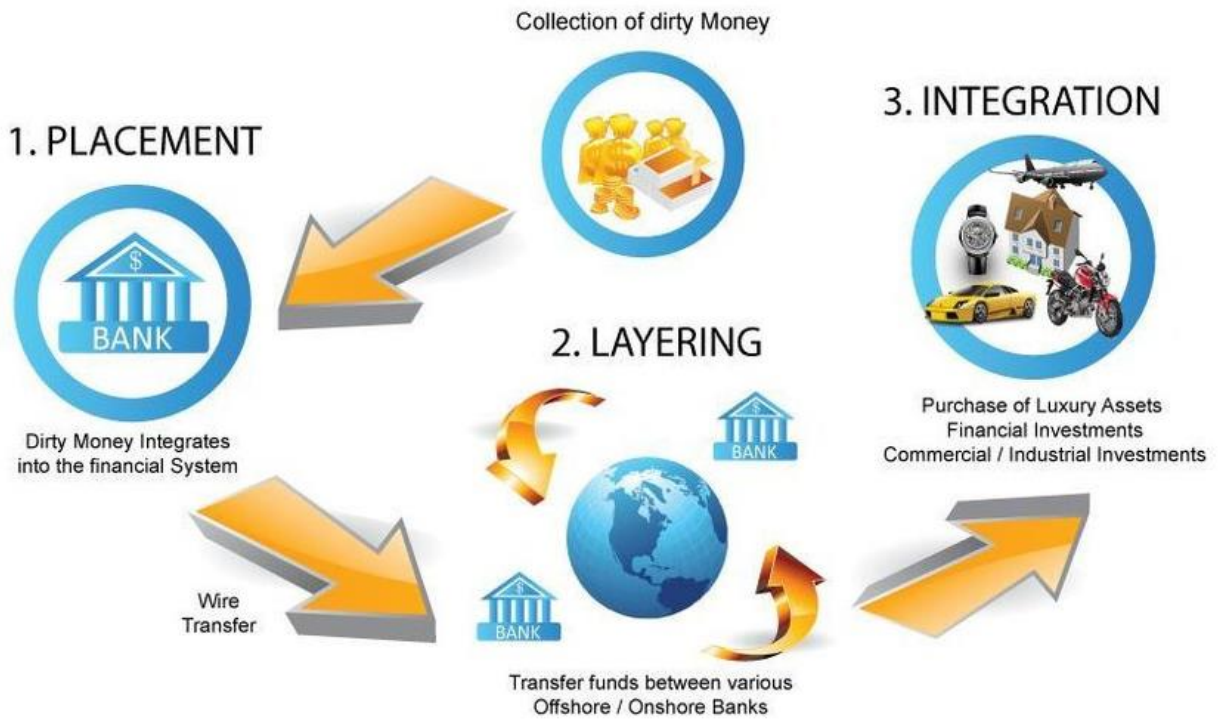
B. Layering

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. *As the next step to the example indicated in A above, such proceeds from the sale are used to buy shares in a legitimate entity or to buy other precious metals and stones 'legitimately' for further resale… these activities further distance such proceeds from its initial illicit activities.*

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 main stages of ML.



DPMS, as part of their risk assessment process, should assess the ML/TF/PF vulnerabilities and high-risk factors associated with each of their products/services. The risk assessment guidance section herein also avails indicators of potential high risks. Such should be duly considered when conducting risk assessments.

5.1 Evolving Nature of the Diamond Trade

DPMS need to keep abreast of changes in their respective trade and industry as such changes can impact ML/TF risk levels. The diamond industry for one has seen drastic changes which have greatly impacted risks. A FATF and EGMONT study[7] indicates that the diamond trade has developed unique culture and trade practices, which have their own characteristics and variations across countries and continents, including the following:

[7] FATF and Egmont Study, Oct 2013.

a. De Beers no longer holds the same all inclusive diamonds monopoly. The activities are now spread across different stakeholders in different countries. This naturally spreads risks which may have been concentrated in De Beers;
b. A number of smaller diamond dealers have entered the market. Their level of risk management systems might not be the same (nor as effective as that of De Beers) thus inherently increasing risk exposure to all stakeholders they deal with;
c. Distribution channels have become more diverse, requiring stakeholders to be aware of risks that may come with all such different channels;
d. New trade centres have emerged with billions of dollars' worth of diamonds, and financial transactions go in and out of newly founded bourses and their ancillary financial institutions;
e. Cutting and polishing has shifted (except for the most valuable stones) from prior known bases in Belgium, Israel and the United States mainly to emerging markets such as India and China, with smaller cutting centres emerging in other parts of the world. Namibia’s local diamond cutting and polishing sector has grown since independence;
f. Cash transactions are still prevalent but the usage of cash is diminishing, thus further reducing risk exposure naturally; and
g. The internet, as in all other facets of life, is rapidly taking its place as a diamonds trading platform. There is enhanced anonymity or reduced levels of verifications with most such platforms, which increases risk exposure.

In all other sectors of precious metals and stones, changes will naturally occur which requires DPMS to review their understanding of risks and if need be, align accordingly.

6. TF RISKS IN DPMS

While the 2012 National Risk Assessment (NRA), 2017/18 update and 2020 NRA rightly observed that ML risks are more frequent and prominent, TF and similarly PF risks cannot be overlooked. It is well established that ML control vulnerabilities can be equally exploited to advance TF or PF activities. For this reason, controls that may be traditionally

viewed as necessary for ML are equally essential for preventing and combatting TF and PF activities. This section speaks to TF risk considerations which are also similar for PF.

Advancing potential TF and PF through DPMS is not new and there has been many findings of such over the years. BBC News reported as far back as 20 February 2003[8] that *"Several members of al-Qaeda's inner circle bought gems in Liberia and from Revolutionary United Front (RUF) rebels in Sierra Leone, according to research first published by the Washington Post. The move into diamonds came as al-Qaeda's assets were frozen. Much of the evidence comes from Western intelligence reports and from the trials of al-Qaeda suspects after the 11 September attacks and the bombings of US embassies in East Africa."* According to Global Witness' estimation al-Qaeda laundered USD 20m through purchasing diamonds.

6.1 Nature of TF

As mentioned herein above, the characteristics of TF can make it difficult to identify. The methods used to monitor ML can also be used for TF, as the movement of TF funds often relies on similar methods (control vulnerabilities) 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)

The risks associated with TF are highly dynamic. As such, DPMS 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

[8] https://dwfgroup.com/en/news-and-insights/insights/2019/1/proposed-aml-and-cft-regulatory-regime

transaction monitoring systems that incorporate dynamic TF risks, along the more static risks associated with ML. The above considerations are similar for PF.

6.2 Transnational[9] 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, DPMS 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 DPMS equally have an obligation to combat PF.

6.3 Namibia as a Conduit for TF

Despite the absence of domestic terrorism, the enhanced TF risks associated with foreign clients, especially those from high-risk countries, who are involved in precious metals and stones cannot be overemphasized. One of the potential consequences of transnational ML is that channels may be established that may also be exploited by terrorist and proliferation 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 DPMSs can be abused to advance TF are similar for PF. The due diligence and RBA, especially screening of clients/parties

[9] Extending or operating across national boundaries

to transactions against sanctions lists is essential in combatting both TF and PF within the sector.

6.4 Nature/Sources of TF funds

Funds that are used in TF (and PF) 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 or proliferation organisation. Where funds are derived from criminal activity, the traditional monitoring mechanisms that are used to identify ML (as explained in this Guidance and Guidance Note 09 of 2023) 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.

6.5 Value/Size of Funds in 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 impact/risk with regard to ML. This is a bigger challenge for DPMS that do not naturally deal in financial 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 DPMS' AM/CFT policy/procedures have to deliberately distinguish controls aimed at detecting potential TF.

6.6 Covert Nature of TF Suspicions

The actions of those supporting terrorist and proliferation activities may be overt (openly) and outwardly innocent in appearance, such as the purchase of shell, or shelf[10] 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

[10] "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.

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 not easy 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 DPMS to *determine the type of underlying criminal activity or intended terrorist, nor proliferation purpose* as a pre-requisite for reporting TF or PF suspicions. The DPMS' role is to simply identify, report the suspicion without delay, freeze any funds or assets of such subject, while treating same with the necessary sensitivity. The FIC and relevant Law Enforcement Authorities have the responsibility to investigate the matter further and determine if there is actual link to terrorism or proliferation activities. The misguided view to first want to establish an actual link to terrorism before filing any report has often exposed us to risks and not helped combating authorities to respond timely and promptly.

6.7 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[11], Faith Based Organizations (FBOs) were identified as the high-risk sub-sector within NPOs. Internationally, charities are largely identified as higher risk NPOs. Though this may rarely happen, DPMS need to apply the necessary level of due diligence when availing their services or dealing in one way or the other with NPOs, especially the types of NPOs specified herein to be higher risk for TF.

[11] 2020 NRA.

Amongst other controls, DPMS have to ensure due identification of ultimate beneficial owners 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.

6.8 Potential Origins 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 DPMS should consider:

a. *Overseas groups able to inspire support through ideology* – Individuals may be inspired to contribute to overseas-based 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. Precious metals can be a source for raising funds or themselves easily transmitted or smuggled to where they are needed. This is the overarching context to keep in mind for TF purposes;
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 known 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.

DPMS 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 move or raise funds to advance TF.

6.9 Helpfulness of ML controls for TF

There are both similarities and differences in the application of the RBA to TF and PF on the one hand and ML on the other. 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 DPMS sector. This does not however mean the sector is not vulnerable to such abuse[12]. The international trade of precious metals and stones, given their exposure to foreign clients, some of whom may have ties to high terrorism risk jurisdictions or have ties to terrorist organizations, remains inherently[13] vulnerable to TF abuse.

7. UNDERSTANDING THE RISK BASED APPROACH (RBA)

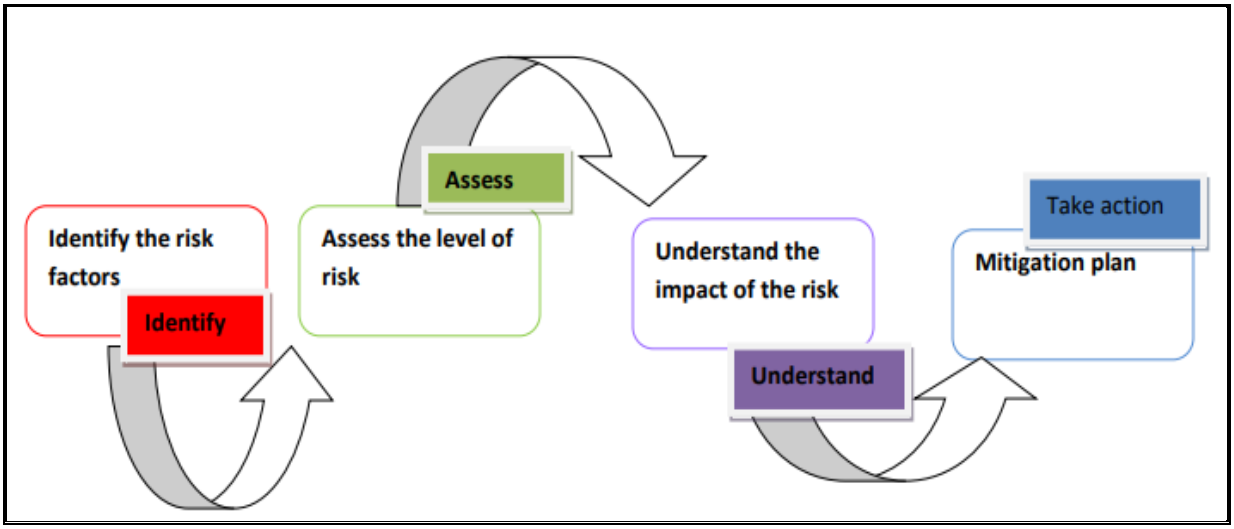
The basic intent behind the DPMS' FIA obligations as derived from international obligations, is to ensure that DPMS' services and operations are not abused for facilitating criminal activities and ML/TF/PF. The limitation of compliance obligations to cash transactions above the threshold as stated herein above already suggests alignment to the RBA.

The RBA speaks to a control system premised on a DPMS' 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

[12] ESAAMLG study also confirms that although the study has not conclusively confirmed a linkage between TF and proceeds of illicit dealing in PMS in the ESAAMLG region and in particular rubies in Northern Mozambique, the possibility cannot completely be ruled out as there are other studies by various researchers who have drawn linkages between rubies and TF. No information was provided by Mozambique that could have helped in establishing a link or none thereof between the illicit dealing in PMS and TF activities.

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

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 DPMS:* 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/PF risks. Guidance Note 09 of 2023, issued along with this guidance explains how to implement risk based controls on the understanding of relevant risks;
c. *Ongoing monitoring:* putting in place policies, procedures and information systems to monitor changes to ML/TF/PF 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/PF 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.

8. FOUNDATION OF THE RBA: CONDUCTING RISK ASSESSMENTS

The object of understanding client and transaction risks is to help the DPMS determine the level of due diligence such client and transaction 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 DPMS needs to gain in reducing its ML/TF/PF risk exposure.

Annexures A - C of this Guidance lists certain indicators which impact ML/TF risk levels of precious metals and stones with some going beyond cash transactions. Though FIA compliance obligations only arise with cash transactions, it is helpful that DPMS understand non-cash payment variables which may expose them to higher risks. It is within this context that guidance and risk indicators herein will also highlight non-cash payment methods[14] which present high risks.

DPMS, like all other sectors 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.

[14] The FATF 2013 Study equally advocates for such approach.

8.1 Undertaking ML/TF/PF Risk Assessments[15]

The 2020 NRA rated the sector's ML vulnerability as Medium High. Unlike sectors rated Very Low to Low, this rating places the sector amongst the sectors which need to ensure effective risk mitigation. In the eastern and southern African region[16], eleven countries that conducted NRAs rated the DPMS sectoral ML risk between Medium and High. Namibia's risk consideration level is thus aligned to most risk levels in the region.

The comprehensiveness of risk assessments should be aligned to the nature, complexity and risk exposure of a DPMS' operations, in view of its products and services (or amendments to such). ML/TF/PF risks can be organised into the following three categories: (a) client risk profiles (b) risks associated with products/services and delivery channels; as well as (c) country/geographic risks. The risks and red flags listed in each category herein below are not exhaustive but provide a starting point for DPMS to use when assessing risks or designing their RBA.

8.1.1 Evaluating Client Risk Profiles

In the examples given below, the client, within the context of this Guidance also includes the counterparty. Such client maybe acting in their personal capacity or could be representing a trust or legal person. The following key risk factors impact a client's ML/TF/PF risk profile for DPMS:

a. Higher Risk Indicators for Counterparties[17] (or clients)

[15] 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.

[16] ESAAMLG Study, March 2022.

[17] can be the customer or person working with or associated with the customer.

Care needs to be taken when dealing with higher risk counterparties to transactions at any level of the value chain/trade. Higher risk counterparties include persons who:

- *do not understand the industry in which he/she proposes to deal, or is not familiar with trade practices (all stages of the trade);*
- *do not have a place of business or equipment or finances necessary and appropriate for such engagement, or does not seem to know usual financial terms and conditions;*
- *proposes a transaction that makes no sense, or that is excessive, given the circumstances, in amount, or quality, or potential profit;*
- *has significant and unexplained geographic distance from the dealer in precious metals or stones;*
- *uses banks[18] that are not specialised in or do not regularly provide services in such areas, and are not associated in any way with the location of the counterparty and the products;*
- *makes frequent and unexplained changes in bank accounts, especially among banks in other countries;*
- *return of an advanced payment from a third party;*
- *receiving/transferring funds for import/export where the ordering customer/beneficiary is a Money Service Business or such higher risk business;*
- *use of third parties to deposit funds into single or multiple DPMS' accounts;*
- *name of sender in the payment transfer to the DPMS is not the importer/buyer (mainly rough and polished trade);*
- *name of receiver in the payment from the DPMS is not the exporter/supplier;*
- *involves third parties in transactions, either as payers or recipients of payment or product, without apparent legitimate business purpose. Includes receiving/transferring funds for import/export activity to/from entities that are not known to be involved in the specific trade of such stones or metals (either an individual or a legal entity);*

[18] though only cash transactions give rise to compliance obligations.

- *use of third parties to sell diamonds, jewellery, stones etc., where this is not acceptable in terms of trade practices (all stages);*
- *will not identify beneficial owners or those with controlling interests in involved legal persons or trusts, where this would be commercially expected (unreasonable secrecy and anonymity);*
- *seeks anonymity by conducting ordinary business through accountants, lawyers, or other intermediaries;*
- *uses cash in its transactions with the DPMS, or with his own counterparties in a non-standard manner. The more cash is used, the higher the risk; and*
- *uses money service businesses or other non-bank financial institutions which present inherently higher risk for no apparent legitimate business purpose. The ESAAMLG study observed that regionally, proceeds from precious metals and stones are laundered in the domestic economies through the real estate sector; mining sector (by reinvesting in the sector); automotive industry; construction industry, tourism sector and the financial sector and its related industries. Any links to these sectors by clients or counterparties thus generally increase ML risk exposure for a DPMS.*

b. ***Politically Exposed Persons (PEPs)*** [19] ***:*** *This includes both domestic and international (PEPs). All PEPs are inherently high risk for ML/TF. PF risk is not excluded. Amongst a host of similar reports, in 2015* [20] *, Customs officers in Bangladesh caught a North Korean diplomat trying to smuggle an estimated USD 1.4m (£ 922,000.00) worth of gold into the country, after a flight from Singapore. Comparatively, foreign PEPs naturally present a higher risk than domestic PEPs as their CDD information cannot*[21] *be effectively or readily verified with relevant domestic authorities. PEPs need to be subjected to Enhanced Customer Due Diligence (EDD)*

[19] 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.

[20] https://www.theguardian.com/world/2015/mar/06/north-korean-diplomat-gold-dhaka-airport-bangladesh

[21] 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.

which include obtaining management approval before facilitating deals involving them, as per FIC Guidance Note 01 of 2019 and Guidance Note 09 of 2023;

Profile mismatch

At times, the profile of the client might not match the values of funds client transacts 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 thus appears to be a front-man for foreign nationals from countries in northern Africa with higher terrorism activities, who are also closely associated with his radicalised 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)

c. Retail Customer Risk

A retail customer (end user) of precious metals or precious stones (especially jewellery consumers) will, in general not have a business purpose for a purchase of an article of jewellery, a precious stone or metal. A purchase is likely to be made for purely personal and emotional reasons that cannot be factored into an AML/CFT/CPF risk assessment. Higher risk can however be seen in certain retail customer transaction methods such as:

- *Use of large amounts of cash. It should be recognized however, that many persons desire anonymity in jewellery purchases for purely personal reasons, or at least the absence of paper records, with no criminal intentions;*
- *Payment by or delivery to third parties. However, not all third party payments are indicative of ML/TF activities. It is relatively common in jewellery purchases that*

a woman will select an article of jewellery, and a man will later make payment and direct delivery to the woman; and

- *Structuring or breaking down into numerous transactions when a single transaction could suffice.*

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 or a relationship starts, 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.

8.1.2 Products, Services and Associated Delivery Channels

An overall risk assessment should also include a determination of the potential risks presented by products and services offered by the DPMS. Delivery channels include methods of conducting the transaction, such as transferring goods, funds etc. Such determination should include a consideration of the following non-exhaustive list of factors:

a. ***Fluctuating value of precious metals and stones:*** *All diamonds, jewels, and precious metals can potentially be used for ML and TF, but the utility and consequent level of risk are likely to vary depending on the value of the product. Unless transactions involve very large quantities, lower value products are likely to carry less risk than higher value products. However, dealers must be aware that values can be volatile dependent upon supply and demand. Relative values of some materials can vary dramatically between different countries and over time;*

b. ***Delayed determination of payment method:*** *In many cases with diamond trade, the form of payment will determine the AML/CFT duties, it may be the case that*

the CDD/KYC and reporting duties will be conducted long after transaction took place and the diamonds have been delivered to the customer. Since diamonds are a form of currency and may be used themselves for ML/TF purposes, this creates a vulnerability in which the ML/TF process may have taken place long before the details of the customer were verified and a report was sent to the relevant FIU;

c. ***Nature of commodity and pricing:*** *Dependent upon the nature of the transaction, counterparties and quantities, gold can be higher risk. Pure gold, or relatively pure gold, is the same substance worldwide, with a worldwide price standard published daily, and it can also be used as currency itself, e.g by hawalas[22]. Gold is available in a variety of forms, e.g bars, coins, jewellery, or scrap, and trades internationally in all of these forms. Price variance in commodities can be abused;*

d. ***Challenges associated with smuggling:*** *Despite controls put in place by authorities and mining companies, the smuggling of precious metals and stones, especially diamonds, remain a problem. In the FATF Study[23] on diamonds, South Africa, as a participating country in the study, indicated that once the smuggled stones have entered or left a country, they are virtually impossible to trace;*

e. ***Commingling:*** *Once precious metals and stones are stolen (for diamonds - whether rough or polished, loose or mounted) in most cases the offender will have to reinsert them into the legitimate trade in order to receive a pay-off. The same is true for illegally mined diamonds, which, in many cases, will be reinserted into the trade through another diamond mine. Thus, commingling of diamonds is actually part of the ML/TF process and every stage of the "diamond pipeline" is vulnerable to commingling;*

[22] Hawala is an ancient money transfer system that is based on personal relationships between the individuals involved in transactions. It moves money (or value) from party to party outside of the traditional banking system. The term "hawala" means "transfer" in Arabic. A "hawaladar" is the broker who facilitates the movement of money. The hawala system can be (and has been) utilized by criminal organizations to transfer funds in or out of a country with little notice by law enforcement. Because of this, Hawala money transfers are unregulated and while it's legal in certain jurisdictions, it may be illegal in others. In India and Pakistan, for example, using systems of trade like hawala is deemed illegal.

[23] FATF Study Oct 2013.

f. ***Risks from uncertainties in values of some units:*** *Although scrap gold alloys or other gold-bearing scrap may require substantial processing and refining to reach an end market, the costs may be discounted in advance, and the scrap may still trade for high value in multi-billion dollar worldwide markets. Values of many scrap materials are uncertain and not precisely knowable until they have been processed and assayed, which can present risks if the parties undervalue or overvalue international shipments;*

g. ***Risks of informality:*** *Alluvial gold and gold dust can be indicative of informal mining by individuals and small groups, often in areas that are characterized by informal banking and absence of regulation and so may present higher risk;*

h. ***Physical characteristics:*** *The physical characteristics of the products offered are also a factor to consider. Products that are easily portable and which are unlikely to draw the attention of law enforcement are at greater risk of being used in cross border smuggling or money laundering. For example, diamonds are small, light in weight, not detected by metal detectors and a very large value can be easily concealed;*

i. ***Trading platform as a means to launder funds:*** *Since it has no advertising overheads and gets customers through word of mouth, it may save consumers up to 40% from retail prices. It is relatively easy for a criminal or money launderers/terrorism financiers to establish online trading platforms to disguise the source of funds;*

j. ***Laundering stolen diamonds via the "Darknet":*** *In spite of not being a common activity, “Silk Road” offered jewellery with diamonds of unknown origin. They could be purchased and paid in Bitcoins (Annexure A cautions around risks associated with cryptocurrencies/assets). Deliveries could be made by Fedex or any other courier service in a plain packages without a description of the goods inside.*

k. ***Dealing in stolen or ill-gotten products or potential fraud at any stage in the value chain:*** *the risk of dealing in stolen or fraudulent products must be taken into account. As with all valuable objects, diamonds, jewels and precious metals are attractive to thieves and dealers must be aware of the risks of trading in stolen products. For example, jewellery dealers, pawn shops and buyers of used gold jewellery should remain alert to the possibility of being offered stolen products or jewellery. In addition to stolen goods, DPMS should be aware of the risks associated with fraudulent goods, such as synthetic diamonds represented as natural diamonds, or 14 karat gold represented as 18 karat. A FATF Report identified that the main vulnerability of the retail level fraud can be divided into several types such as:*

- *False grading: where a metal or stone's true grade is not reflected in the nominated grading;*
- *False certificates: where a grading certificate has been counterfeited, subject to unauthorised amendment, duplicated and attached to stones/metals of varying quality;*
- *Misrepresentation of stone/metal: where other non-legitimate stones/metals are passed off as legitimates;*
- *Non-disclosure of type: where synthetic stones like diamonds and fracture-filled diamonds are not declared as such and are passed off as undamaged, naturally-mined diamonds; and*
- *Valuation fraud: where a stone is undervalued to avoid customs duty and/or tax, or to advance transfer pricing.*

l. ***Services offered:*** *Major gold dealers for example create metal accounts for their customers, for temporary secure storage or for investment and they transfer counterparties' gold credits in these accounts among themselves, and among repositories and delivery destinations worldwide, with services comparable to those provided by banks with money and financial credits. Such services, by banks as well as by major gold dealers, may be useful to money launderers and terrorist financiers to move high values through international commerce, under the guise of*

legitimate business, but are unlikely to be anonymous and irregular, and thus may be considered lower risk;

m. ***Inconsistencies or anomalies with industry practices including:***

- *When the origin/destination of funds differs from the destination/origin of the stones or metals (e.g mainly rough trade and polished trade);*
- *The appearance of rare stone/metal (diamonds) in the international market outside of known trading procedures (e.g., Argyle's rare pink diamond appearing in the international marketplace outside of the annual tender process (rough trade, cutting and polishing);*
- *Selling or buying precious metals and stones between two local companies through an intermediary located abroad (lack of business justification. uncertainty as to actual passage of goods between the companies);*
- *Purchase of precious metals and stones with a credit card issued in a country which is not the buyer's country (where credit cards are used, mainly retail); and*
- *Regular interval purchases, rather than seasonal purchases from foreign wholesaler (retail especially, less so with diamond dealers and wholesalers).*

Practical Money Laundering

Money launderers want to get as much as possible of their illegal assets out of these transactions. They may be prepared to accept losses in these layering transactions, but may prefer to keep them to a minimum. Therefore, transactions involving high value product and low transaction costs may be particularly attractive to money launderers and terrorist financiers.

For example, a purchase of pure gold coins, and subsequent sale of those coins at another location, will quickly return most of the original purchase price. On the other hand, a purchase of a specialty gold alloy may have a resale value of only the gold content, losing any value added in manufacturing, and losing gold refining charges as well. Such a transaction will cause criminals to pay substantial transaction costs and may therefore lower overall risk.

n. *Risk impact from **financing methods**: The method of payment used may affect the ML/TF risk level. The following are worth noting:*

- ***Involvement of financial institutions may reduce risks:** The risks are likely to be reduced if transactions take place through the mainstream banking system, as banks would have subjected the movement of such funds and clients to some form of due diligence. Conversely, the risks may increase when payments do not originate from financial institutions;*

- ***Cash enhances risks:** The main methods of payment used by dealers are wire transfers or electronic funds transfer. Cash, especially in large amounts, can be a warning sign, especially if the use of such cash is anonymous or intentionally hides an identity, e.g the true purchaser funds the transaction by giving cash to a third party, who then becomes the nominal and identified purchaser;*

- ***Third parties:** Payments or delivery of product to or from third party accounts, e.g accounts in the names of persons other than approved counterparties;*

- ***Unrelated activities (unusual patterns):** Payments to or from accounts at financial institutions that are unrelated to a transaction or approved counterparties, such as banks located in countries other than the location of the counterparty or transaction.*

8.1.3 Considering Country or Geographic Risk

Some countries and geographic locations are of greater AML/CFT/CPF concern but the risk level in a given transaction can increase or reduce - dependent on elements of a transaction, including: (1) where a product is mined; (2) where a product is refined or finished; (3) location of a seller; (4) location of a purchaser; (5) location of the delivery of a product and (6) location of funds being used in the transaction. Within this context, factors that should be considered in determining a given country's risk level include:

a. ***Known industry controls/regulations:*** *For rough diamonds, a producing or trading country which participates in the Kimberley Process is expected to have reasonable measures to help mitigate risks. Counterparties or clients from countries which are highly regulated does not automatically mean that all risks are low. To be given such a lower risk consideration, a client or counterparty should have a compliance program and demonstrate to be in compliance with its applicable regulatory system;*

b. ***Unjustified source origin of precious metals and stones:*** *Whether there is known mining or substantial trading of the transaction product – diamonds, jewels or precious metals - in a transaction source country. If it is clear that the cited country of origin does not produce such metal or stone, there may be enhanced risks. This also includes considerations whether a country would be an anticipated source of large stocks of existing diamonds, jewels or precious metals, based upon national wealth, trading practices and culture (centres of stone or jewel trading, such as Antwerp, Belgium) or unanticipated (large amounts of old gold jewellery in poor developing countries). It should be recognized, however, that gold and silver have cultural and economic significance in a number of developing countries, and very poor people may have, buy and sell these metals;*

c. ***Access to markets and value adding operations:*** *Whether there is ready access from a country to nearby competitive markets or processing operations, e.g. gold mined in Africa is more frequently refined in South Africa, the Middle East or Europe rather than in the United States, and a proposal to refine African gold in the United States would be unusual and higher risk;*

d. ***High risk jurisdictions:*** *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 as ***not having effective AML/CFT/CPF measures*** *in place;*

- *identified to be* ***uncooperative in extraditions and providing beneficial ownership information*** *to competent authorities, a determination which may be established from reviewing FATF Mutual Evaluation reports or reports by organisations that also consider various co-operation levels such as the OECD Global Forum reports on compliance with international tax transparency standards;*

- ***Identified higher risk countries:*** *this may include conflict zones, countries subject to sanctions, embargoes issued by the international community including the UN, OFAC, EU etc. Also includes FATF greylisting or blacklisting. South Africa, potentially Namibia's largest trading partner and a country cited in the 2020 domestic NRA as a primary international ML outlet/corridor has well publicized mushrooming of illegal miners (known as Zama-Zamas) in precious metals and stones. Stones and metals, including dealers from such country may naturally present higher risks.*

  The ESAAMLG study revealed that the destination of the illicitly traded precious metals and stones is within the region and outside the continent. In the region, the destination countries were listed as South Africa, Botswana, Uganda, Tanzania, Zambia, and Mozambique and that these were in most instances used as transit destinations. The United Arab Emirates, China, Russia, Thailand, Belgium, USA and India were the commonly cited countries outside the region. The preferred mode of moving precious metals and stones was by road, for the countries in the region and by air and sea for those outside the region. DPMS should thus apply the necessary due diligence and care when dealings have ties to these jurisdictions.

- *identified as **providing funding or support for terrorist activities** or that have designated terrorist organisations operating within them, especially in small and **artisan mining areas**;*

- *with an **extensive use of cash** in trade or its economy. Cash intensive economies/countries have inherently higher risks;*

- *with **significant informal banking systems** operating in the country, e.g hawalas operate in many developing countries; and*

- *identified as having **significant levels of organised crime, bribery, corruption, tax evasion, capital flight, or other criminal activity**, including being a major source or a major transit country for illegal drugs, human trafficking and smuggling as well as illegal gambling. Care needs to be taken when such is observed within neighbouring states of clients involved in deals given the crossborder nature of some of these crimes.*

The DPMS' 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 practical risk considerations for each foreign client or delivery channel, geographic link etc.

8.1.4 Trade Based Money Laundering (TBML) Risks

DPMS are an easier means to advance TBML. One of the main methods through which TBML is conducted is by way of over or under valuation. The diamond industry is tremendously vulnerable to TBML primarily because of the high subjectivity in the valuation of diamonds, the ability of diamonds to change their form, the trade and global nature of the diamond market and the long production chain involving many actors.

To compound the problem, there is no commodity or market price or "price list" for diamonds since there is no specific product. With respect to parcels of bulk diamonds,

which may include different diamonds of different sizes and quality, it is impossible and impractical for the evaluator to examine each and every diamond that is set for export and thus can be easily overvalued or undervalued to facilitate TBML schemes. Below is an example of TBML in developing countries:

Practical TBML & Transfer Pricing

Authorities have noted how products such as gold, but especially diamonds sold may be shipped from one jurisdiction to another and be assigned low value to minimize inland revenue or export duties, then traded in the other jurisdiction or re-exported from it with a much higher "price tag". This is how typical TBML may occur in the DPMS industry.

Transfer Pricing risk is higher within the diamond industry as it includes multinational companies with operations spanning across many countries, serving as trade centres of rough and polished diamonds. The term 'transfer pricing' is usually used in the context of tax regimes where related companies (subsidiaries, affiliates) conduct international transaction between themselves. Simply put, revenues can be shifted to another country with preferred or lower regulation or tax rates.

By way of over or under invoicing with affiliate diamond companies located in Free Trade Zones (FTZ), it is possible to illegitimately shift profits from diamond companies in high tax rate countries to FTZs and thus avoid taxes. It is also possible to use the same scheme for ML/TF purposes. The combination of a lack of transparency in the diamond trade with a lack of transparency in a FTZ provides an excellent atmosphere to conduct large volume transactions without detection.

8.1.5 Variables Which Reduce (or change) Risk Determination

To design a RBA methodology, there must be deliberate measures to identify lower risks for application. Below are considerations which reduce risk levels:

a. *The size of the transaction, with larger transactions presenting higher risk and the opposite being true as well;*

b. There may be no or limited regulation when a product is mined and sold for the first time, but the level of regulation may increase as the product continues to be traded;

c. The regularity or duration of the business relationship, or of general knowledge of the counterparty's role in the industry. Longstanding relationships involving frequent contact provide an understanding of a counterparty's legitimacy within the dealer's industry, and information by which a proposed transaction can be evaluated for consistency with industry norms;

d. The level of government regulation of counterparty's business and accounting practices reduces risks. Companies and their wholly owned subsidiaries that are publicly owned and traded on a regulated exchange, or that have publicly issued financial instruments, generally pose minimal risks. Note however that this is not always so, and publicly traded companies may be established by money launderers;

e. Some governments are also involved in transactions through export and import regulatory systems, often for the purpose of collecting taxes or duties, which require traders to describe their materials and declare values and counterparties of export or import. Such government involvements may lower risk;

f. Gold is traded worldwide in very large amounts in direct physical transactions and through financial derivatives, i.e. forwards and futures, which can be used to acquire and sell rights in physical gold stocks. Such paper gold transactions, of any size, are highly unlikely to be anonymous or conducted in cash, certainly in regulated markets and probably in unregulated markets, but should not be ignored for AML/CFT purposes;

g. A large proportion of rough diamond sales are made through Belgium, which strictly regulates dealers and transactions (including the physical inspection and value assessment of all imported and exported diamonds, hence for instance excluding valuation and synthetic diamonds related risks), and through bourses with stringent membership rules of practice;

h. Systems of dealer warranties and transactions through bourses further reduce risk in the trade of polished diamonds and jewellery containing diamonds, as do dealings with only bank transfer payments among regulated and government supervised dealers.

8.2 Increase in illegal mining and dealing cases

There has been an increase in cases of potential illicit dealings in precious metals and stones. The high profile case allegedly involving persons working in the office of the Minister of Mines and Energy widely reported on in 2022 shows potential abuse of office in awarding prospecting licenses to Chinese mining entities. This mater is before court at the time of reporting. Another case in southern Namibia shows how rouge law enforcement officers are at the centre of illegal mining of precious stones and metals. Police have acted[24] to arrest and charge suspects in this matter in the months of May and June 2023.

8.2.1 Illegal lithium mining activities

Below is a summarised version of the suspected illegal Lithium mining case as reported[25] by the local media:

Government officials linked to a controversial N$50 million lithium mining deal

The use of lithium has grown significantly given its essential value to electric vehicles. It is an essential element in manufacturing batteries for electric cars. The growth in such cars, given the green economy drive has increased the demand for lithium globally. China, being one of the largest producers of electric cars naturally has a high demand for lithium.

It was reported that three officials are accused of playing a role in removing businessman Jacobus de Klerk from claims to a mine near Uis, about 120km northwest of Omaruru, and handing control of the rich deposits to a Chinese-owned firm, Xinfeng Investments.

The suspected three officials connected to the transaction are Rafael ‘Ralph’ Muyamba, a former Technical Assistant to the Minister of Mines and Enerrgy, Timoteus Mashuna, a

[24] https://www.namibian.com.na/11-suspected-illegal-miners-arrested/
[25] https://namibian.com.na/the-n50m-lithium-mine-heist-2/ also see the New Era Newspaper of 08 June 2023

historian in the Ministry of Defence and Veterans Affairs. The third official is Ndili Benyamen, a Geologist at the Ministry of Mines and Energy, and a friend of Mashuna.

De Klerk says he was tricked into surrendering his claims while he was healing from a medical condition. The officials are suspected of using their relatives and associates to apply for mining claims in areas with high-value minerals, especially where there is interest from foreign mining companies. These claims are mainly those that are about to expire and where little or no substantial exploration work is carried out. It was reported that government officials irregularly shared information with these companies to ensure they are awarded such rights. In essence what happened suggests his entity failed to re-apply for exploration rights which were reaching expiry date and a group of highly connected persons may have abused their positions to sell of such exploration rights to a Chinese mining firm.

Developments in this case as per filed court papers point to potential organised criminal syndicates in the mining sector. The *New Era* newspaper on 08 June 2023 reported that due process at BIPA may not have been followed in amending the founding statements of Orange River Mining Exploration CC. Previously, Gideon Smith owned 85% of the said CC with Peter Shifwaku owning a 15% stake. Peter Shifwaku is a cousin of the Minister's former Technical Assistant, Mr Muyamba. The said amendments resulted in Shifwaku owning 100% interest in the said CC, with Gideon Smith not featuring anywhere in the ownership structure. Court papers further suggests that Gideon's consent, through signing the said amendments was never sought. It is indicated that his signature may have been fraudulently copied and pasted onto the CC2 amended founding documents. BIPA, as an applicant in the matter is reported to be accusing Shifwaku of falsifying the said documents. The *New Era* further reported that the first payment was NAD 16 million on the date of signing the agreement, followed by another NAD 16 million on the transfer date and a final payment of NAD 16 million was transferred on the closing date. BIPA has since suspended two officials suspected of possibly facilitating the said fraudulent amendment of CC documents.

Court documents show that Shifwaku agreed to sell his newly acquired 100% interest in Orange River Mining Exploration CC to Xinfeng for NAD 50 million on 23 June 2022. The payment was made through Shifwaku's Orange River Mining Exploration CC. The Chinese

company also agreed to pay Shifwaku NAD 6 million upon signing the agreement. That same month, Shifwaku's mining company splashed money on eight vehicles – a Ford Ranger worth NAD 1,1 million, Volkswagen Amarok valued at NAD 933 400, a top-of-the-range Toyota Hilux Legend worth NAD 819 000, three Volkswagen Tiguans worth NAD 639 900 each, and two other Toyota Hilux Legends worth about NAD 500 000 each. Bank statements show payments of NAD 50 000 to NAD 400 000 were transferred to people believed to be Muyamba's associates or relatives.

Muyamba resigned from his post in April 2022 in the wake of this matter being exposed and law enforcement commencing investigations in the deal. The Minister of Mines and Energy, Tom Alweendo reported him to the Anti-Corruption Commission in March or April 2022 and in a subsequent media briefing, distanced himself from the alleged corruption.

As adviser to Alweendo, Muyamba held an influential position. *The Namibian* further reported Mr Muyamba saying that: "If my cousin is benefiting and is earning an income out of that, what can I do?" "He is my cousin. The law does not say if you work at the ministry your cousin should not benefit." "The law is very clear that me and my wife and children cannot benefit. I don't have a wife. My children are not beneficiaries of those mineral rights". He further said his brother Josef Muyamba has had mining interests for over eight years.

HOW IT MAY HAVE HAPPENED …

De Klerk previously told *The Namibian* that he was swindled out off his company Karlowa Mineral Resources by business associates while he was in hospital recovering from head injuries caused by a car accident. De Klerk's mining claims expired while he was in hospital and were not renewed, that is a counter argument by some at the Ministry of Mines and Energy.

De Klerk said his employee, Isak Shoombe, introduced him to Mashuna, Benyamen, and Thomas Alfeus. "Thomas pretended to be the answer with all connections everywhere. He introduced me to Mashuna and Ndili (Benyamen). I had no idea it was a scam," he said. He spent about nine months in hospital in 2016. That is when Mashuna, Benyamen and his wife

Albertina Ekandjo reportedly removed him from the company and took charge of the mining claims.

Karlowa Mineral Resources' registration document bears the names of Ekandjo, Mashuna and the late businessman Barnabas Ugwanga. It was during this time he claims he was removed from Karlowa Mineral Resources' documents as both shareholder and director.

As a result, De Klerk lost his mining claims for zinc, tantalum and lithium. The claims were allegedly transferred to a new entity called Karlowa Mining Enterprise. Mashuna is the sole director of this entity, with company registration documents stating he co-owns it with Immanuel Shoopala Iipanda, Hosea Isak Shoombe, and Tomas Alfeus. Records show that the four at one point served as directors in Karlowa Mineral Resources with Ekandjo and De Klerk. Benyamen confirmed knowing De Klerk, but denied any involvement by his wife.

Mines executive director Simeon Negumbo told *The Namibian* in February 2021 that De Klerk had four mining rights which he held from 10 November 2013 to 9 November 2015. He confirmed that those claims were awarded to Karlowa Mining Enterprise, because De Klerk did not renew them. De Klerk says he was in hospital and unable to do so.

Xinfeng, which now owns the lithium mine, is developing a reputation of being on the wrong side of the law in Namibia, reported *The Namibian* newspaper. As this was unfolding, Alweendo announced that he has stopped the company from exporting lithium ore because the company had failed to honour its legal obligation to process the mineral in Namibia. He said the company claimed that the 54 000 tonnes exported to China were test samples. As the company imported 80 Chinese tipper trucks to transport the ore to the harbour, doubts emerged over whether the company has any intentions of building a processing plant in Namibia. Earlier, *The Namibian* reported that mining commissioner Shivolo stopped Xingfeng's mining explorations after the company started mining without an environmental clearance certificate.

Notable Red Flags:

Predicate offences of corruption and bribery in authorities: *The Ministry of Mines and Energy, as regulatory and licensing authority has had reports of potential corruption, fraud and general bribery, mostly involving people in positions of authority;*

Using front companies and persons: *Ministry officials and highly connected persons potentially using front companies and hiding their beneficial ownership through relatives and associates;*

Lack of due diligence, encouraging non-compliance: *The involved Chinese company has been at the centre of reports suggesting potential illicit activities and gross non-compliance. Authorities entrusted with ensuring compliance have not acted. The inadequacies in mining inspections to ensure compliance could be a contributing factor. Seeing allegations herein, there are indications that authorities are in bed with rouge companies. At the time of reporting on this matter, the said company was also facing challenges related to potential non-compliance with tax laws;*

Abuse of company secretarial services: *The changing of beneficial owners in the said companies to facilitate the potential illegal activities is a classic typology of how changing owners/directors renders legal persons (companies) highly vulnerable to abuse. Note that CCs are highly abused in this syndicate and the 2023 NRA update suggests CCs are high risk for ML; and*

Integrity breaches at BIPA: *in this case, the suspected unlawful amendment of CC documents to facilitate changes in beneficial owners of Orange River Mining Exploration CC could not have happened without integrity breaches at BIPA. It is reported that the BIPA CEO had reversed such alleged unlawful amendment, but her reversal was challenged in court. The two BIPA officials suspected of having assisted in the commission of this illicit activity were suspended.*

8.2.2 Illegal mining of precious stones

One of the major challenges faced by the Ministry of Mines and Energy is the inadequate resources for inspections and such related due diligence around areas susceptible to illegal mining activities. If mining and prospecting inspections or relevant due diligence is not effective, the risk of illegal mining activities is escalated. Below is another case showing an increase in illegal mining activities in Namibia.

Law Enforcement Officers at the centre of an illegal mining syndicate

A Law Enforcement Officer based in southern Namibia around areas surrounding precious stones and metals may have been running an illegal mining syndicate. It is suspected that the minerals may have been sold locally (to a less extent), with most of them possibly sold in neighbouring South Africa. South Africa has an established underground industry for dealings in illegal mining and trading in precious stones and metals. The case is still under investigation and the suspected proceeds observed thus far are below NAD 5 million.

Blue Lace Agate is a precious stone found on the farm Ysterputs 254 (meaning iron holes) in Namibia. The mine is located adjacent to the “Blinkpan” (shining shallow lake) which can be seen to the west of the B1 highway about 80 km north of Vioolsdrift and Noordoewer, which are the border towns on either side of the Orange River between South African and Namibia[26]. At the time of this publication, the matter is still under investigation and below are a few indicators observed to date:

a. **Illegal mining:** There is no evidence that these mining activities are duly licensed. The suspected buyers of precious stones from such activities do not appear to question the legitimacy of their origin (indications of legitimate mining operations), as would be expected;

[26] http://namibianbluelace.co.za/about/

b. **Foreign buyers:** The suspected buyers are mainly South Africans with some Chinese residing in Namibia also potentially buying from these ringleaders;

c. Suspicious payment trends:

- Payments are received from or made to, all types of persons or entities, if their account descriptions are anything to go by. There is record of bank accounts belonging to medical entities; entities selling timber, spare parts, steel; Chinese construction firms; one or two schoolteachers etc. Their role, if any, in these links is unclear at this stage;
- Ringleaders appear to be using bank accounts of their relatives, family and children to conduct transactions, receive large payments etc. This clearly shows disparity between account holder profile and transacting behaviour;
- Some of the ringleaders, whose sole financial profiles/sources of income suggests salary they receive as law enforcement officers, appears to be trading in financial values way beyond their established profiles;
- Small funds transfers via mobile wallets appear to be made to other law enforcement officers by the recipient of suspicious proceeds. This may suggest more law enforcement officers could have been involved in one way or the other;
- Funds received into local accounts are immediately disbursed to ringleaders or suspected miners accounts who further swiftly dispose-off funds by way of ewallets/transfers/POS purchases;
- New bank accounts are opened and large funds transferred to such new bank accounts before withdrawals and transfers/spend. See below observations around account irregularity:
    - ✓ In some cases, such accounts receiving huge amounts were previously inactive;
    - ✓ In most cases, funds are almost depleted the moment such funds are received through withdrawals and transfers to various people;
    - ✓ Clients would transfer funds from their most commonly used bank accounts held at some of the biggest banks to their accounts held at other or smaller banks that are hardly active. This could potentially reduce risk of detection as the new banks may not know the expected behaviour or client profile;

- ✓ When an account to which funds are transferred is in overdraft and the account holder continues to use the funds for purchases, transfers, and creditor payments. The account overdraft facility makes it difficult for law enforcement to seize the tainted funds.

- In some instances, payments to the ringleaders are referenced with the intended recipient's name and narration 'stone/s', suggesting a direct link;
- Associates, (or possibly runners) or members of the organised crime were paid using mobile banking apps, especially ewallets, P2Cs etc. There is record of ATM withdrawals and POS purchases in South Africa by persons who have received proceeds from the ringleaders; and
- Large cross border payments from South Africa received into individual's accounts.

d. **Abuse of modern payment systems:** Payments to the ringleaders suggest transfers from South African banks. In some instances, these would be transfers using modern banking Apps, EFTs etc;

e. **Hidden assets:** Suspects do not appear to have vehicles registered in their names but they appear to have been paying for vehicles if their bank account records are anything to go by. Large deposits or initial payments would be paid via bank transfers and it would be made to appear as if the rest is paid through monthly instalments. Also, ringleaders appear to have comingled illicit proceeds with payments for stock or inventory possibly for their grocery store. There are further indications of building material purchases suspected to be for one ringleader possibly renovating or building apartments; and

f. **Potential mine employees' involvement:** Persons suspected to be associated with or employed at Blinkpan Mine appear to be receiving and transferring funds from/to the suspected ringleaders of the organised crime syndicate. This may suggest that they are selling precious stones to the ringleaders.

Notable Red Flags:

Failure to report suspicious transactions: *Despite the suspicious transacting behaviour (transactions outside established client profiles) stated herein above, most banks did not detect such and report same to the FIC timely, as per the FIA;*

Lack of due diligence: *mine employees operate in high risk environments. The risk of theft is high. It is expected that considerations around employee due diligence should detect irregular employee activities or conduct. The involved Chinese company has been at the centre of reports suggesting potential illicit activities. Authorities entrusted with ensuring compliance have not acted. Seeing allegations herein, there are indications that authorities are in bed with rouge companies; and*

Cross border smuggling of minerals: *Though not proven, it is highly suspected that the precious stones are smuggled out of Namibia, into South Africa, via the porous border. The method of such operation is not yet clear at this stage. The ease with which people cross the border at unofficial points along the Namibian-South African border is a major concern (2020 NRA). The potential for corrupt customs officials playing a hand in the cross border smuggling, though seen in other cases, was not yet established in this case.*

8.3 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 DPMS. If such partnerships exists, the DPMS that still owns the precious metals and stones 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.

8.4 Type, Nature and Extent of Controls

The aim of managing risks in business is to reduce inherent[27] risks to tolerable or acceptable residual[28] levels. DPMS 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.

8.5 External Risk Assessments

The considerations and indicators herein are not exhaustive. DPMS are required to consider observations from SRA and NRA reports issued by the FIC. Local[29] and international trends and typology reports issued by bodies such as ESAAMLG[30] and FATF[31] (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 some local and international publications. ML and TF trends are dynamic, it is thus essential to keep abreast of updated publications in this regard.

Relying on other relevant industry measures such as the Kimberly Process should always be considered as long as it can avail effective risk mitigation for ML, TF and PF activities.

8.6 Risk Assessment/Management Reports

All identified risks as far as clients, transactions and geographic considerations are concerned should be documented in Risk Management Reports. Such report(s)

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

(assessment outcomes) should be periodically updated when material changes arise in risks and controls.

9. 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 DPMS. DPMS are further required to duly study Guidance Note 09 of 2023, amongst others, which speaks to the practical implementation of controls to mitigate ML/TF/PF risks at institutional level.

The FIC website contains several other Directives, Guidance Notes, Circulars and Regulations which avail helpful guidance on measures to combat ML/TF/PF in terms of the FIA.

10. 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.

11. NON-COMPLIANCE WITH THIS GUIDANCE

This document is a guide. Effective implementation is the sole responsibility of DPMS. 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 deemed effective by the FIC as supervisory authority implementing the FIA.

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

DATE ISSUED: 12 JUNE 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

ANNEXURE A

GENERAL INDICATORS[32] IMPACTING ML/TF RISKS

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/PF purposes. Below are results from the 2023 NRA update showing how ML threats exploited 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 CCs: *The 2023 NRA update suggests that CCs are* ***the most abused type of legal persons*** *in terms of financial values[33]. 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.*

[32] FIC Observations and risk assessments
[33] As per cases analysed by the FIC and referred to various investigative authorities on findings that suggest possible ML.

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

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[34] 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.*

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

b. *Complex ownership or legal structure:* *Should be viewed along with observations above. Clients where the 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. Unexplained use of **shell and/or shelf companies, front companies**, legal entities with ownership through nominee shares or bearer shares, control through nominee or corporate directors, legal persons or legal arrangements splitting company incorporation and asset administration over different countries, all without any apparent legal or legitimate tax, business, economic or other reason;*

*ii. **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*

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

DPMS need to be cautious with unusual complexity in control or ownership structures without a clear explanation, where there are certain transactions, structures, geographical location, international activities or other factors not consistent with the DPMS' understanding of the client's business or economic purpose behind the dealing in precious metals and stones.

c. *High risk of non-face-to-face clients or beneficial owners:* *Should also 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, when such is possible and perhaps reasonable or who provide instructions intermittently without legitimate reasons and are otherwise evasive or very difficult to reach, when this would not normally be expected;*

- *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).*

All such circumstances/clients should be subjected to EDD as explained in Guidance Note 09 of 2023.

d. ***Known convicts or persons charged with proceed generating crimes:*** *Clients with previous convictions for crimes that generated proceeds, who instruct DPMS (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;*

e. ***Unusually high offer for products/commodities:*** *The offer by client/counterparty to pay extraordinarily higher fees for products, which would not ordinarily warrant such a premium, present higher risks. Also, when client or counterparties show no concerns around prices unreasonably higher than valuation, it may be a red flag as launderers are often prepared to lose some or minimal funds in order to launder most of their proceeds.*

f. ***Misalignments in proposed and actual activities:*** *when actual/real activities of the company (as customer/counterparty) are unclear or different from the stated purposes in the incorporation documents or internal regulations of the company, trust deed or foundation, risk exposure is increased.*

g. ***False information (or evasiveness):*** *when the person giving instructions to the DPMS is reluctant to provide all the relevant information or the DPMS has reasonable grounds to suspect that the provided information is incorrect or insufficient. Reluctance (or unconvincing explanation) to explain source of funds is a red flag. If a DPMS' 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 previously known financial position and the buyer cannot explain the reason*

for their increased funds. DPMS' customer's level and/or source of wealth may be inconsistent with their circumstances. Such transactions/services should be subjected to EDD as per Guidance Note 09 of 2023;

h. ***Exposure to Cryptocurrencies:*** *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.*

i. ***Risks associated with NPOs:*** *Though dealing with NPOs may not be common for DPMS, care needs to be taken when such transactions arise. It is generally accepted that some NPOs are highly vulnerable to TF. The 2020 NRA found Faith Based Organisations (FBOs), in particular those associated with radical or extremist Islam, to be most vulnerable to TF. Persons who display such extremist tendencies may present higher TF risks. Internationally, charity organisations are found to be most vulnerable to TF abuse. This naturally also exposes Namibia to enhanced TF risks associated with charities, especially given the global reach of some. DPMS 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;*

j. ***Inexplicable or unreasonable company or ownership changes:*** *changes in client ownership increase risk exposure to the DPMS. Especially when the legal structure has been altered frequently and/or without logical reason (e.g. name changes, transfer of ownership, change of beneficiaries, change of trustees, change of partners, change*

of directors or officers). Frequent or unexplained change of professional adviser(s) or members of management can be a red flag. Global publications also suggest that the unreasonable transfer of the official headquarters or 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, transfer pricing, tax evasion etc.;

k. ***Indications of non-compliance:*** *Indicators that client does not wish to obtain necessary governmental approvals, comply with local or international frameworks in place suggest higher risks;*

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

m. ***Unreasonable and undue pressure to expedite sale/services:*** *Clients or counterparties who request that transactions be completed in unusually tight or accelerated timeframes without a reasonable explanation for accelerating the transaction. This makes it difficult or impossible for DPMS to perform a proper risk assessment or due diligence;*

n. ***Unexpected resuscitation:*** *Sudden activity from a previously dormant client or counterparty without a clear explanation may suggest potential higher risks. May suggest that they could be used by others to deal on their behalf;*

o. ***Attempts to facilitate, advance, support or commit illicit activities:*** *Any attempt by the counterparty, 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;*

p. ***Request to vouch on behalf of client:*** *Services where DPMS 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;*

q. ***Links to higher risk services/activities:*** *Links with non-bank financial mechanisms such as currency exchange businesses or money remitters, which are generally higher risk for ML/TF;*

r. ***Use of pooled client funds:*** *at times, various clients can pool funds together and have one or some of them use such to purchase. Pooled client funds or assets, without justification or legitimate business reasons often increases risk as funds could be pooled from illegitimate sources;*

s. ***Use of multiple accounts:*** *When client uses multiple accounts at several financial institutions for no logical reason, it can be suspicious as they may be trying to structure huge amounts/transactions with different institutions. In some cases, DPMS 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;*

t. ***Unreasonably 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.*

ANNEXURE B

RISK INDICATORS FOR FINANCIAL INSTITUTIONS AND DPMS

Most of the following relate to trade financing vulnerabilities:

a. ***Uses of "IOUs"[35] or promissory notes:*** *promissory notes are used to cover debts related to the trade of diamonds (especially in bulk) by miners, dealers, brokers, cutters and polishers. They are negotiable instruments – as opposed to IOUs, which are non-negotiable instruments – and can be treated in the same way as cash (i.e transferrable to a third party). The free and unrecorded circulation of these mostly honoured IOUs creates an unofficial and unmonitored "banking system", that provides financing for traders, outside the official banking system.*

   Furthermore, in most circumstances, the circulation of the promissory notes is totally "in house" within the "guild" of diamonds especially. The actual financial risk of a diamond dealer is "under the radar" of the official banking creditors and regulators. The unrecorded circulation of IOUs facilitates the transfer of high value assets, without a trace in the monitored financial system. Thus, it is possible to cause the transfer of largescale funds, just by word of mouth among two persons who are members of Diamonds exchanges in different and remote locations. The unrecorded circulation of IOUs facilitates the transfer of high value assets, without a trace in the monitored financial system, hence escalation of risk;

b. ***Memo transactions:*** *memo transactions may bear some vulnerability to misuse in terms of ML/TF. These vulnerabilities are linked to possible variation of the prices of the diamonds evaluated, over or undervalued, and to the possibility of fraud committed by the consignee. For example, a potential buyer may review a parcel of precious stones and metals and select some of the stones while returning*

[35] Investopedia defines an IOU, as a phonetic acronym of the words "I owe you," … as a document that acknowledges the existence of a debt. An IOU is often viewed as an informal written agreement rather than a legally binding commitment. An IOU between two people conducting business may be followed up with a more formal written agreement.

the unsold ones to the consignor. The original shipment may occur at a certain stated value while the unsold return is made at another value (potentially over or undervalued). This flexible gap of value is common and may not be considered unusual or suspicious by the financial institution. But it may also be used for ML purposes. The difference in price also raises the question whether the stones returned were all included in the shipment in the beginning. It has to be noted that the percentage of returns of polished diamonds is high.

In certain cases that involve familiar and reliable diamond dealer account holders, some banks do transfer funds or accept funds as advance payment without any document agreement (save for a statement by the diamond dealer account holder), and then monitor the advance payment. The bank may be limited in the ability to verify that the financial transactions correspond to the terms of the memo and the value of the diamonds. The other risk linked to memo transactions is the possibility for fraud, when the consignee does not return the diamonds consigned.

c. ***Advance payment:*** *some of the accepted* ***financial*** *practices by DPMS (especially diamond dealers) may also serve as conduit to ML or TF. For one, it is an accepted practice to transfer funds as an advanced payment for the stones. These are payments conducted without sending the precious stones. In many cases the advanced payment is returned back to the customer/diamond dealer. These transactions may be used to send back money from a third party and thus create what could seem an audit trail for proceeds from illicit activities;*

d. ***Return shipments:*** *another accepted practice which create a ML/TF vulnerability is the return of shipments (partial or hole). In transaction such as memo transactions, stones/metals are sent to the customer for his review and in case the customer is not satisfied with the stones/metals he will send some or all them back to the dealer. This in many cases would be accompanied with a return of funds already paid. Banks financing the trade would need to be aware that the funds should be returned from the same party to which the funds were initially transferred*

to and also with the same value. This may also be relevant to the dealer where his customer is asking to transfer or transferring such funds to a third party;

e. ***Fork Transactions:*** *in general these are transactions where funds are sent/received to/from other parties then those appearing in the documents as customer/supplier;*

f. ***Date of Sale vs Date of Payment:*** *while conducting a transaction, the dealer and its customer (which may also be another dealer) will negotiate the terms of the deal including terms of payment. In most cases the stones/metals will be provided close to the date of the sale and before the payment is received. The date of payment may be upon delivery of the diamonds but may also be several months later.*

ANNEXURE C

INDICATORS FOR CUSTOMS AUTHORITIES

Red flags related to export/import (documentation and entities involved)

a. *Origin of diamonds or other precious stones and metals seems to be fictitious;*
b. *The long validity period of the KP Certificate or such relevant permits/supporting document opens up possibilities for reuse and setting up a carousel;*
c. *Low invoice amount: might be structured to reduce related import/export duties or costs, could also be to advance TBML or transfer pricing;*
d. *Overvaluation of imported good;*
e. *The consignee does not specify a permanent address on the airway bill but makes use of a hotel, or other temporary accommodation, to receive the shipment, complicating the audit trail;*
f. *The consignee specified on the airway bill is a known dealer, but a different delivery address is provided;*
g. *The diamond or such other precious metal and stone appears to have been shipped as a form of payment.*

ANNEXURE D

VULNERABILITY ENHANCING FACTORS

Criminals seek to retain control over criminally derived funds or assets while evading law enforcement's ability to trace the origin and ownership of such ill-gotten funds or assets. Various FIC publications show the many ways criminals launder money. It may involve acting in concert with other individuals, businesses and companies. However, one constant remains: The ill-gotten assets or funds need to be washed or somehow presented as though they originate from a legitimate source. Laundering is premised on distancing illicit assets from their criminal origin. Characteristics which make precious stones and metals attractive to criminals are their:

a. ***Value-to-mass ratio;***

b. ***Ability to retain value over time****;*

c. *Ability to maintain* ***or carry significant value in small and easily transportable*** *quantities;*

d. ***Non-traceability****: once the items change hands and enter the licit market they are difficult to trace, in terms of both their original ownership and value. Additionally, with diamonds, once they have gone through the beneficiation process and the rough diamonds are cut and polished, it becomes almost impossible to determine the origin of a stone, since Kimberley process only applies to rough diamonds;*

e. ***Ability to remain unmarked*** *throughout the value chain - It is virtually impossible to distinguish between precious metals (e.g rough diamonds) that were illegally obtained and those that were legally obtained. Technology allows for the marking of diamonds so it would be possible to follow the trail of the diamonds, i.e. who is involved in the sale/purchase of the diamonds, however, most diamonds are unmarked. Diamonds are also easily disguised as other stones of much lesser*

value. The use of diamond simulants and synthetics can be used to commit frauds (predicate offence). Diamond marking can mitigate the risk of ML/TF the more it comes into practice and if documentation of the transactions include this data;

f. *Ability **easily buy and sell commodities outside the formal banking system:** AML/CFT measures are higher in the formal banking systems, but transactions can be conducted outside this system and the value is carried between countries without having to go through the KYC procedures in the banking sector. Also, most precious stones and metals can be bought and sold in all parts of the world at almost any jewellery or pawn shop;*

g. *Ability to function as a **means for exchange**: The use of some precious stones and metals as currency has been noted in some parts of the world. Because diamonds display a high value-to-weight ratio, retain their value and are not affected by inflation or exchange rates, they are used in exchange for other commodities or forms of currency. Some criminal organizations have been said to use such as forms of payments in illicit trades or debt settlements. Similarly, proceeds from the legal or illegal sale of diamonds can be used to finance terrorism and proliferation activities. Diamonds can have similar characteristics as cash. In terms of ML/TF vulnerabilities, this is a particularly important feature since diamonds are not included in the concept of cash/currency or a bearer negotiable instrument (FATF recommendation 32) even though it is possible to both launder with diamonds themselves and use diamonds as a means of payment to finance criminal activity, e.g. for the purpose of buying drugs or paying for illegal arms.*