NBFIRA

Non-Bank Financial
Institutions Regulatory
Authority

CONDUCTING AN INSTITUTIONAL RISK ASSESSMENT

AML/CFT/P Guidance Note 4
for Non-Bank Financial Institutions

Effective January 1, 2024

Disclaimer

This Guidance Note is issued by the NBFIRA in line with section 49(1)c of the Financial Intelligence Act and Regulations 2022 (“FI Legislation”) of the Republic of Botswana for comprehensive use by the NBFIs. The note is indicative and while due care was exercised to ensure that its contents are accurate and consistent with the FI Legislation, the latter shall prevail in the unfortunate case of ambiguity and the NBFIRA does not guarantee or take any liability whatsoever.

Contents

1. AUTHORITY, PURPOSE AND SCOPE

(a) Authority

This *Guidance Note* is issued by the Non-Bank Financial Institutions Regulatory Authority (NBFIRA), pursuant to its authority as provided for in Section 49 (1) (c) of the Financial Intelligence Act, 2022 (FI Act), which empowers the Authority to issue instructions or guidelines to help non-bank financial institutions (NBFIs) comply with the FI Act. They are also issued pursuant to the authority as provided for in Section 53(1) of the Non-Bank Financial Institutions Regulatory Authority Act of 2023 (NBFIRA Act).

(b) Purpose

The purpose of this *Guidance Note* is to lay out the procedures for identifying, assessing, and mitigating money laundering, terrorism financing, and proliferation financing risks in line with the requirements of Section 13 (1) of the FI Act. It requires NBFIs to identify, assess and understand money laundering, terrorist financing and proliferation financing risks they face and should act and apply resources aimed at ensuring the risks are effectively mitigated.

(c) Scope

This *Guidance Note* applies to institutions licensed/exempted and supervised by the NBFIRA through various primary legislation and secondary legislation. These include, among others, the NBFIRA Act, Insurance Industry Act, Retirement Funds Act, Botswana Stock Exchange Act, Collective Investment Undertakings, the Securities Act, Virtual Assets Service Providers Act.

2. ACCOUNTABILITY AND RESPONSIBILITY

Section 14 (1) (e) of the FI Act states that NBFIs *shall implement programmes which have regard to the risks identified in its risk assessment, commensurate to the size of the business and shall in that regard - implement and maintain a customer acceptance policy, internal rules, programmes, policies, processes, procedures or such controls as may be prescribed to protect its system from financial offences.* This is to ensure, as stated under section 13 (8) that neither an NBFI *nor a service offered by it, is* *capable of being used by a person to commit or to facilitate the commission of a financial offence.*

To this end, the boards of directors [or senior management in the absence of the former] of NBFIs are accountable and responsible for their entity's compliance with provisions of the FI Act, including assessing the risk of commission of financial offences and taking appropriate measures to manage and mitigate the identified risks relating to business relationships, pre-existing products, practices, and delivery mechanisms, new technologies, geographical locations, new business procedures and product delivery channels. The responsibility may be delegated to executive management to ensure compliance during day-to-day business activities as conducted by an NBFI.

3. DEFINITIONS OF TERMS USED IN THE GUIDELINES

Financial Action Task Force (FATF) - Is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognized as the global anti-money laundering (AML) and counter terrorist and proliferation financing (CTFP) standard.

Specified Party - A person listed in schedule I of the Financial Intelligence Act, 2022.

Risk – The likelihood of an event and its consequences. In the context of money laundering/terrorist financing (ML/TF), risk means:

- *At the national level*: threats and vulnerabilities presented by ML/TF that put at risk the integrity of Botswana's financial system and the safety and security of the country.

- *At the reporting entity level*: threats and vulnerabilities that put the reporting entity at risk of being used to facilitate ML/TF.

Threat – Person or group of people, an object, or an activity with the potential to cause harm. In the ML/TF context, a threat could be criminals, facilitators, their funds or even terrorist groups.

Vulnerability – Elements of a business that may be exploited by the threat or that may support or facilitate its activities. In the ML/TF context, vulnerabilities could be weak controls within a reporting entity, offering high risk products or services, etc.

Consequence – The impact or harm that ML/TF/PF may cause, such as the impact on reputation and imposition of regulatory sanctions.

Impact: this refers to the seriousness of the damage that would occur if the ML/TF risk materialises (i.e., threats and vulnerabilities).

Risk Based Approach – An approach whereby competent authorities and firms identify, assess, and understand the ML/TF/PF risks to which they are exposed to and take AML/CFT/CFP measures commensurate to the identified risks to mitigate them effectively.

***Risk Factors* –** Means variables that, either on their own or in combination, may increase or decrease the ML/TF/PF risk posed by an individual business relationship or occasional transaction.

Risk Management – The process that includes the recognition of ML/TF/PF risks, the assessment of these risks, and the development of methods to manage and mitigate the risks that have been identified.

Inherent Risk – The intrinsic risk of an event or circumstance that exists before the application of controls or mitigation measures.

Residual Risk – The level of risk that remains after the implementation of mitigation measures and controls.

Likelihood – The chance of the risk being present.

4. INTRODUCTION

Money laundering is a serious economic threat to the country’s financial system and can have negative consequences at national, sectoral and institutional level. Non-compliance with AML/CFT regulations can expose the reporting entity to significant regulatory and reputational damage. As such, effective anti-money laundering systems need to be designed to be able to detect and prevent money laundering and the financing of terrorism and proliferation in financial institutions. The institutional ML/TF/PF Risk Assessment is one of the tools intended to prevent reporting entities from being exposed to the proceeds of crime, terrorist financing, proliferation financing and other financial crimes

5. BACKGROUND

(a) A well-developed risk assessment assists in identifying an institution’s ML, TF and PF risk profile. Understanding the risk profile enables the entity to apply appropriate risk management processes to the Anti-Money Laundering /Combating the Financing of Terrorism/Combating the Financing of Proliferation (AML/CFT/CFP) compliance program to mitigate the risks.

(b) The risk assessment should provide a comprehensive analysis of the ML/TF risks in a concise and organised presentation and should be shared and communicated with all business lines across the entity, board of directors and management.

(c) There is no universally agreed and accepted risk assessment methodology by either governments or institutions, which prescribes the nature and extent of a risk assessment. Accordingly, this *Guidance Note* seeks to articulate relevant considerations which NBFIs may find useful in developing and implementing a reasonably designed institutional risk assessment. The specifics of an institution’s particular risk identification process should be determined by each institution based on their operations.

6. RISK ASSESSMENT

(a) Risk is generally defined as the possibility and impact of an uncertain event on an object. Uncertainty comes because of threats (external factors), vulnerability (internal weakness relative to external threats) and consequence (impact if risk occurs). In this context, the risk would refer to the possibility of financial crimes and their impact given the vulnerability of a NBFI.

(b) An institutional ML/TF/PF risk assessment can be defined as a process of identification, assessment and understanding of risks at institutional level to determine the risk level of financial crime on their operations and related party activities, thus the threats, vulnerabilities, and possible impact. A risk assessment is the foundation of a proportionate risk-based AML/CFT/CPF framework.

(c) The Financial Action Task Force (FATF) requires countries and financial institutions to identify, assess and understand ML/TF/PF risks they face and take appropriate action. Moreover, Section 13(1) of the Financial Intelligence Act, 2022 requires that NBFIs should conduct assessment to determine the risk level of financial crime on their operations and related-party activities. In addition, the law specifies areas to be assessed for risks which include businesses practices, relationships and transactions, products, and their delivery channels.

(d) Section 13(4) further states that NBFIs are to document these assessments to be able to demonstrate their basis, keep these assessments up to date, and have appropriate mechanisms to provide risk assessment information to competent authorities and or supervisors upon request.

(e) The context within which specified parties assess ML/TF risks is also influenced by ML/TF risks that are identified at a national level in all the jurisdictions where they operate.

7. ASSESSING ML/TF/PF RISKS

7.1 Identify Threats and Vulnerabilities

(a) The first stage in the risk assessment process is to identify all potential threats that can impact the organisation, then identifying vulnerabilities which can be exploited by the threats. Risk identification requires broad understanding of the market within which the entity is operating, as well as technical aspects of the sector it is part of. It is, therefore, essential to involve all staff members of different professional backgrounds and various divisions to identify most of the potential risks. To provide foundation and direction, this activity should start with desktop research on typologies of financial crimes that can potentially be committed through and within the greater sector and sub-sectors which the entity is part of[1]. Once the hypothetical risks are understood and consolidated from the research, a practical risk identification on the entity and its operating environment should be conducted starting at divisional level building towards consolidated ML/TF/PF risk universe at organisational level.

(b) Identified potential ML threats may include high levels of organised crimes, corruption, wildlife/drug/human trafficking and other proceeds generating crimes (i.e. tax evasion and fraud). For TF and PF threats, these may include political conditions, terrorist activities, illegal development of weapons, political/cultural/business links to designated terror groups and state sponsors or their locations. Other threats may emanate from economic crises and regulatory changes.

(c) Vulnerabilities may include weak internal control structures including staff integrity, controls, minimal or no understanding of ML/TF/PF subject, customer onboarding processes, operational procedures, products/service features or technological infrastructure, acceptance of unlimited cash transactions/bulk cash transactions/third party transactions. Also, dealing with anonymous transactions/accounts, cash intensive businesses, shell and shelf companies,

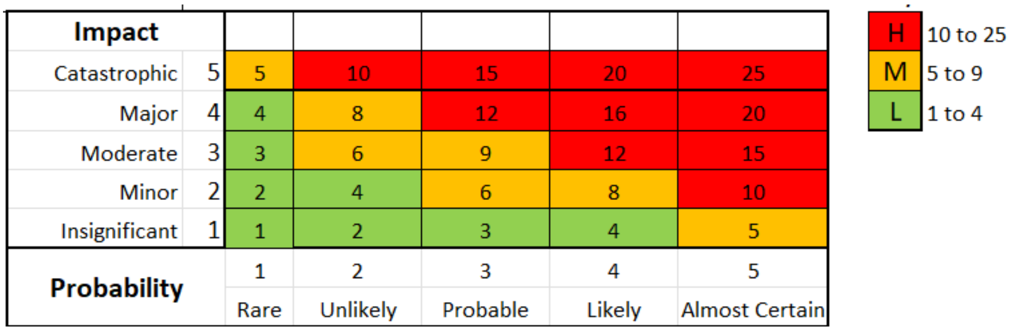
[1] References may include National Risk Assessments reports, other sectoral reports, crime reports etc.

legal entities with complex structures, dealing in high luxury goods may raise the likelihood of abuse for ML/TF/PF.

(d) Having compiled ML/TF/PF risk universe, risks may be rationalised by combining and redrafting similar threats and vulnerabilities or grouping them under sub-headings or categories. Validation should also be conducted to ensure the identified risks are realistic and material.

7.2 Categorise and Prioritise Risks

(a) The second stage is apportionment of identified risks into risk factor categories, usually five – namely, business nature/size, product/service, geographical locations, distribution channels/business practice, and customer base profile then rating them accordingly using a well calibrated risk matrix (likelihood vis-a-vis potential impact). Some of the factors may be apportioned with vulnerabilities only or threats only – or both where reasonably so. For example, geographic location and customer profile may reasonably be about threats since they are external factors, whereas product/service and business practice/delivery channels may be suited for vulnerabilities only since it is an internal factor. Assess each category individually, considering the specific vulnerabilities and threats associated with them.



Impact						
Catastrophic	5	5	10	15	20	25
Major	4	4	8	12	16	20
Moderate	3	3	6	9	12	15
Minor	2	2	4	6	8	10
Insignificant	1	1	2	3	4	5
Probability		1	2	3	4	5
		Rare	Unlikely	Probable	Likely	Almost Certain

H	10 to 25
M	5 to 9
L	1 to 4

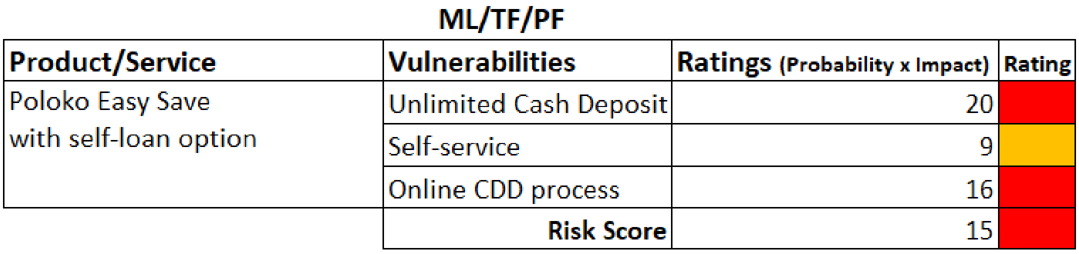
Figure. 1 - Sample Risk Matrix

7.3 Assessing Products and Services Risk

(a) Entities should consider the potential ML/TF & PF associated with each of their specific products or service. An organisation will seek to identify their portfolio of product types and assign an inherent score to each, based on its general inherent characteristics and the degree of ML/TF & PF risks present.

(b) In undertaking this assessment, all products and services should be included in identification of their inherent risks, rationale, mitigation controls, scores, weights, and the residual risk. It is, therefore, important that specified parties can demonstrate how they bring different indicators to bear on a given scenario to reach an appropriate risk classification. Below are some of the factors to consider when doing product risk analysis.

- Does the product enable third parties who are not known to the institution to make use of it?
- Does the product allow for third party payments?
- To what extent does the product provide anonymity to customers?
- To what extent is the usage of the product subject to parameters set by the entity e.g., value limits, duration limits, transaction limits, etc. or to what extent is the usage of the product subject to penalties when certain conditions are not adhered to?
- Does the usage of the product entail structured transactions such as periodic payments at fixed intervals, or does it facilitate an unstructured flow of funds?
- Does the firm understand the risks associated with its new or innovative product or service, in particular, where this involves the use of new technologies or payment methods.
- The reporting entity should determine to what extent are products or services cash intensive e.g., in the case of microlenders.



ML/TF/PF

Product/Service	Vulnerabilities	Ratings (Probability x Impact)	Rating
Poloko Easy Save with self-loan option	Unlimited Cash Deposit	20	🟥
	Self-service	9	🟧
	Online CDD process	16	🟥
	Risk Score	15	🟥

Figure. 2 - Product/Service risk assessment focusing on vulnerabilities

7.4 Assess Delivery (Distribution) Channels Risk

(a) Examine the distribution channels, such as online platforms, branches, and third-party agents.

(b) Identify vulnerabilities related to data security, fraud prevention and compliance within each distribution channel.

(c) Since NBFIs have various modes of transaction and distribution of their products and services, it is equally important to assess whether and to what extent do methods of delivery, such as non-face to face or the involvement of third parties, including intermediaries/agents could increase the inherent risk of ML/TF & PF.

(d) In conducting an institutional risk assessment, NBFIs are required to list all the delivery channels, identify inherent risks, rationale, mitigation/controls, scores, weights used and the residual risk. Some factors to consider include:

- Is the product offered to prospective clients directly or through intermediaries?
- Any agents and or intermediaries the specified party might use and the nature of their relationship with the entity.
- Are prospective clients onboarded through direct interaction or through intermediaries/agents?

- Do clients transact by engaging with the institution directly or through intermediaries/agents?
- Where clients interact through intermediaries/agents, are the intermediaries/agents subject to licensing and/or other regulatory requirements?
- whether the customer physically present for identification purposes. If they are not, whether the firm,

  ❖ Considered if there is a risk that the customer may have sought to avoid face-to-face contact deliberately for reasons other than convenience or incapacity.
  ❖ Used a reliable form of non-face-to-face CDD; and
  ❖ Taken steps to prevent impersonation or identity fraud.

ML/TF/PF

Distribution Channels and Business Practices	**Vulnerabilities**	**Ratings (Probability x Impact)**	**Rating**
Online customer onbording	No verification process	20	🟥
	No customer location limits	16	🟥
	Accept foreign currencies	9	🟨
	Risk Score	**15**	🟥

Figure. 3 - Business practice risk assessment focusing on vulnerabilities

7.5 Assess Geographical Location Risk

(a) Entities should identify domestic and international geographic locations that may pose financial crime risks in their operations. Geographic location risks may also be assessed with respect to the location of customers, business division, line or branch, and may also include its subsidiaries, affiliates, and offices, both domestically and internationally. It is important to consider United Nations Security Council (UNSC) sanctions lists, political conditions, and national and international crime statistics from reputable organisations.

(b) Each case should be evaluated individually when assessing the risks associated with doing business, such as:

- Is the client domiciled in Botswana or in another country or does the client operate/do business in another country?
- Countries that are subject to international sanctions, embargoes or similar measures issued by credible organisations such as the UNSC and the Financial Action Task Force (FATF).
- Countries identified by credible organisations as lacking appropriate AML/CFT laws, regulations, and other measures.
- Any country identified by the FATF as having strategic AML/CFT deficiencies.
- Countries identified by credible sources as providing funding or support for terrorist activities or that have designated terrorist organizations operating within them.
- Countries identified by credible sources as having significant levels of corruption, source of narcotics, human trafficking and other criminal activities.

(c) A rural area where customers are known to the community could present a lesser risk compared to a large urban area where there are different classes of customers with various risks. However, this is not to imply rural areas are inherently low risk, remote areas with proximity to international borders may be prone to other risks such as drug trafficking and influx of foreign currencies. Criminal elements may also choose to stay under the radar in a smaller or less economically active area.

(d) When undertaking this assessment, the institution is required to identify risks and explain the risk scoring allocated to each geographical area highlighted. The assessment should also indicate: Mitigation/ Controls, Scores (Risk Level), Weights used and the Residual Risk.

7.6 Other Qualitative Risk Factors

(a) Entities should also assess additional risk factors that can have an impact on operational risks and contribute to an increasing or decreasing likelihood of breakdowns in key AML/CFT controls. Qualitative risk factors that directly or indirectly affect inherent risk factors may include:

- Significant strategy and operational changes.
- Structure of ownership/ business e.g., presence of subsidiaries.
- National Risk Assessments.

(b) If a reporting entity identifies situations that represent a high risk for ML/TF/PF activities, it should control these risks by implementing mitigation measures.

7.7 Detailed Analysis of The Risks

(a) Once a reporting entity has identified the risk, the next step of the risk assessment process entails a more detailed analysis of the data obtained during the identification stage to accurately assess ML/TF risk.

(b) This step involves evaluating data pertaining to the reporting entity's activities (e.g., number of domestic and international transactions, types of customers, geographic locations of the reporting entity's business area and customer transactions).

(c) This detailed analysis is ultimately important because within any type of product/service or category of customer there will be clients who pose varying levels of risk. This gives management a better understanding of the reporting entity's risk profile in order to develop the appropriate policies, procedures, and processes to mitigate the overall risk.

(d) Additionally, institutions should undertake an impact analysis and develop a likelihood versus impact matrix to help determine the level of effort or monitoring required for the identified inherent risks.

(e) Institutions can also use a risk matrix as a method of assessing risk in order to identify the risk categories that are in the low-risk zone, those that carry somewhat higher, but still acceptable risk, and those that carry a high or unacceptable risk of money laundering and terrorism financing. In classifying the risk, an entity, considering its specificities, may also define additional levels of ML and TF risk. A risk matrix is not static; it changes as the circumstances of the entity change.

7.8 Weights and Scoring

(a) Due to the nature of each institution's unique business activities, products and services (including transactions), client base and geographic footprint, a risk-based approach is used to calculate inherent risks. Each risk factor is usually assigned a score which reflects the associated level of risk. Each risk area may then be assigned a weight which reflects the level of importance in the overall risk calculation relative to other risk areas.

(b) The weight assigned to each of these risk categories (individually or in combination) in assessing the overall risk of potential money laundering may vary from one institution to another, depending on their respective circumstances. Consequently, an institution will have to make its own determination as to the risk weights and scores to assign to the different risk.

7.9 Risk Mitigation

(a) The reporting entity must develop and implement policies and procedures to mitigate the ML/TF/PF risks they have identified through their institutional risk assessments. The mitigation measure should include;

- Internal policies, procedures and controls to fulfil obligations under the FI Act.
- Adequate screening procedures to ensure high standards when hiring employees.
- Ongoing training for officers and employees to make them aware of the laws relating to money laundering, the financing of terrorism or proliferation.
- Policies and procedures to prevent the misuse of technological developments including those related to electronic means of storing and transferring funds or value;
- Mechanisms for preventing money laundering, financing of terrorism or proliferation, or any other serious offence.
- Independent audit arrangements to review and verify compliance with and effectiveness of the measures taken in accordance with the FI Act.
- Risk based approach to managing ML/TF/PF risks identified.
- Customer identification procedures.
- Record keeping and retention.
- Reporting procedures.
- Confidentiality requirements and procedures.
- Transaction monitoring systems; and
- Adequate screening procedures for customers against relevant sanctions lists.
- Enhanced identification, verification and ongoing due diligence procedures with respect to customers who have been identified as high-risk customers.

7.10 Residual Risk

(a) Once both the inherent risk and the effectiveness of the internal control environment have been considered, the residual risk should be determined.

(b) Residual risk is the risk that remains after controls are applied to the inherent risk. It is determined by balancing the level of inherent risk with the overall strength of the risk management activities/controls. The residual risk rating is used to indicate whether the ML/TF risks within the institution are being adequately managed.

(c) It is possible to apply a 3-tier rating scale, to evaluate the residual risk on a scale of High, Moderate and Low. Alternatively, another rating scale could also be used, for example a 5-point scale of Low, Low to Moderate, Moderate, Moderate to High, and High.

7.11 Assessing and Measuring Risks

(a) Once the risks have been identified , each risk needs to be assessed and measured in terms of the chance (likelihood) it will occur and the severity or amount of loss or damage (impact) which may result if it does occur.

(b) The risk level associated with each event is a combination of the likelihood that the event will occur and the impact it could have.

Likelihood x Impact = Risk Level

Likelihood

(i) Likelihood refers to the potential of a particular risk occurring in the business.

(ii) Three levels of likelihood are provided as examples, but there may be more than three for the business.

- ***Very likely***: Almost certain – it will probably occur several times a year
- ***Likely***: High probability it will happen once a year
- ***Unlikely***: Unlikely but not impossible.

(iii) The likelihood levels above may not cover every scenario and are not prescriptive. They may be extended depending on risk management methodology adopted by an entity.

Probability	1	2	3	4	5
	Rare	Unlikely	Probable	Likely	Almost Certain

Figure. 4 - Example of a 5-level Likelihood risk measurement

Impact

(i) Impact refers to the seriousness of the damage which could occur if the risk happens.

(ii) The reporting entity knows its business and is in the best position to know how it would be affected by any impacts. What impacts may affect it and how those impacts would affect it. Some examples of impacts to think about could include:

- How the business would be affected by a financial loss from a crime.
- The risk that a particular transaction may result in a terrorist act and loss of life.
- The risk that a particular transaction may result in funds being used for any of the following: corruption, bribery, tax evasion, drug trafficking, human trafficking, illegal arms trading, terrorism, theft, or fraud.

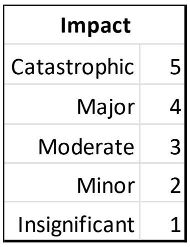
Note that these do not cover every scenario and are not prescriptive.

Three levels of impact are shown here, but the reporting entity can have as many as necessary for its business:

- **Major:** Severe damage
- **Moderate:** Moderate level of damage
- **Minor:** Minimal damage.

(iii) Once an entity assesses the likelihood and impact of each risk, it can then determine the inherent risk level based on these two factors. The following is an example of how a reporting entity can use a risk matrix to determine the inherent risk level posed by customers.

(iv) Similar to likelihood, impact levels may also vary depending on other considerations by an entity.



Impact	
Catastrophic	5
Major	4
Moderate	3
Minor	2
Insignificant	1

Figure. 5 - A 5 level Impact measurement

7.12 Risk Matrix

(a) The risk matrix can be used to combine the *likelihood* and *impact* to obtain a *risk score (inherent risk level)*. The inherent risk level may be used to aid decision making and help in deciding what action to take.

(b) How the inherent risk score is derived can be seen from the risk matrix shown below. Three levels of risks are shown (Low, Medium and High), but there can be more than three, if necessary.

Table 2. Risk Matrix

Likelihood / Impact	**Minor (1)**	**Moderate (2)**	**Major (3)**
Very Likely (3)	Medium 3	High 6	High 9
Likely (2)	Low 2	Medium 4	High 6
Unlikely (1)	Low 1	Low 2	Medium 3

7.13 Apply Controls to Manage Risks

7.13.1 The response/control to the risk will depend on the level of risk as shown in the table below.

Table 3. Response Table

Risk Score	Risk Level	Description & Response	Residual Risk
6 - 9	High	Risk likely to happen and/or to have serious consequences. Response: Do not allow transaction until risk reduced.	Medium
3 - 4	Medium	Possible this could happen and/or have moderate consequences. Response: May go ahead but take steps to reduce risk.	Low
1 - 2	Low	Unlikely to happen and/or have minor or negligible consequences. Response: Okay to go ahead.	Low

7.13.2 This step is about determining how to manage the risks identified and assessed. Managing ML/TF/PF risks involves applying systems and controls. Examples of risk reduction or controls could be;

(a) Setting transaction limits for high-risk products (for example limiting the amounts or frequency of transactions).

(b) Having a management approval process for higher-risk products or customers.

(c) A process to place customers in different risk categories and apply different identification and verification methods.

(d) Rejecting customers who wish to transact with a high-risk country.

The following table provides an example of how the information recorded could be.

Table 4. Example: Customers

Risk	Likelihood	Impact	Risk Score	Control /Action
New customer	Likely	Moderate	2	Standard ID check ID verification type
Customer who brings in large amounts of used notes or small denominations	Likely	Major	3	Non-standard ID check ID verification type

Customer whose business is registered overseas with no office in Botswana	Very Likely	Major	4	Do not accept as a customer

(i) It is important to keep in mind that if a customer, transaction or country is identified as high risk it does not necessarily mean that criminal activity is occurring or will occur.

(ii) The opposite is also true. Just because a customer or transaction is seen as low risk, this does not mean the customer or transaction is not involved in criminal activity. Knowledge of the business and common sense should be applied to the risk management process.

7.14 Monitor and Review

(a) Once documented, the reporting entity should develop a method to regularly evaluate whether its AML/CFT/P programme is working correctly and effectively. If not, it needs to work out what needs to be improved and put changes in place. This will help keep the programme effective and meet the requirements of the FI Act.

(b) Keeping records and regularly doing an evaluation of a reporting entity's risk and AML/CFT/P programme is essential. Risks change over time, for example, changes to the reporting entity's customer base, its products and services, its business practices and the regulatory requirements.

7.15 Continual Improvement

7.15.1 Implement a process for continual improvement by regularly reviewing and updating the risk assessment to adapt to changing threats and vulnerabilities.

7.16 Training and Awareness

7.16.1 Train employees and stakeholders on the importance of risk management and ensure awareness of the institutions risk assessment findings and strategies.

7.17 External Feedback

7.17.1 Seek external feedback from regulators, auditors, and industry peers to gain insights and best practices to enhance your risk assessment process.

8. REPORTING OF MONEY LAUNDERING/ TERRORIST FINANCING/ PROLIFERATION FINANCING RISK ASSESSMENT RESULTS

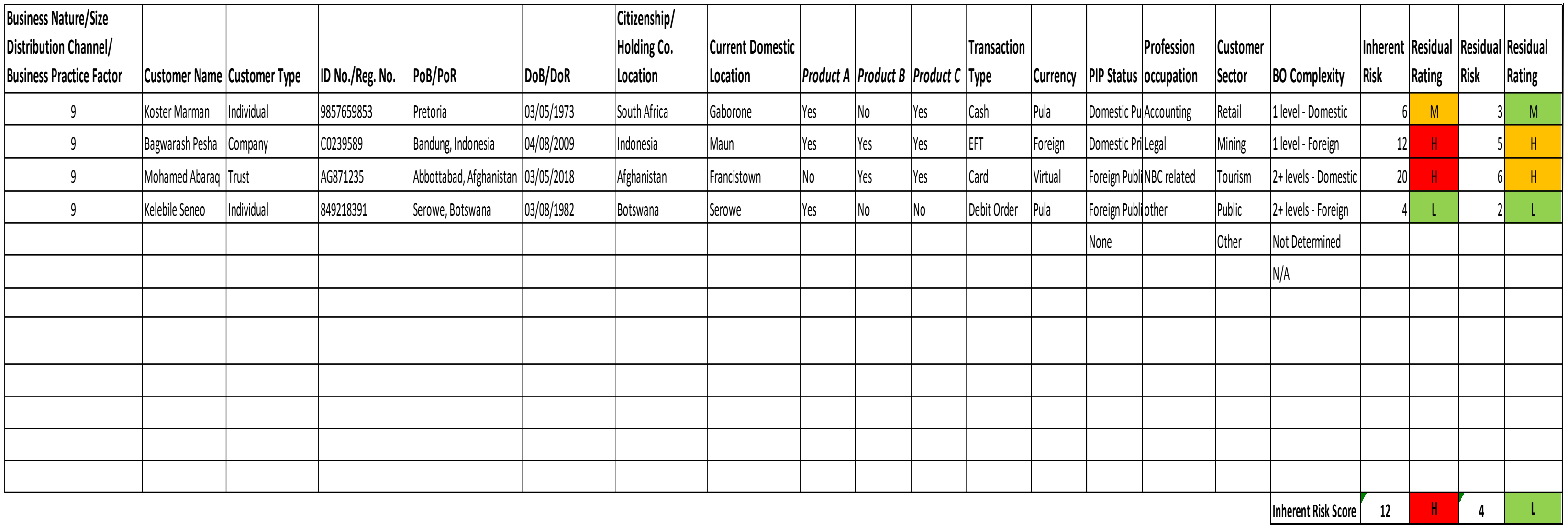
(a) The results of the ML/TF/PF risk assessment should be presented to senior management and the board and communicated by the Compliance Officer to all business units and the control functions of the institution. The report should clearly indicate proposed action points to be adopted by the institution.

(b) The Institutional ML/TF/PF Risk Assessments that will be developed by the NBFIs should be approved and signed off by the board of directors or senior management and be reviewed at such intervals as required by the board or by changes in the regulatory environment. NBFIs shall provide to the supervisory authority a report on the latest results of its MT/TF/PF risk assessment as and when required.

9. AUTHORISATION

9.1 This Guidance Note was approved on January 30, 2024, and it applies immediately.

Annexure



Business Nature/Size Distribution Channel/ Business Practice Factor	Customer Name	Customer Type	ID No./Reg. No.	PoB/PoR	DoB/DoR	Citizenship/ Holding Co. Location	Current Domestic Location	*Product A*	*Product B*	*Product C*	Transaction Type	Currency	PIP Status	Profession occupation	Customer Sector	BO Complexity	Inherent Risk	Residual Rating	Residual Risk	Residual Rating
9	Koster Marman	Individual	9857659853	Pretoria	03/05/1973	South Africa	Gaborone	Yes	No	Yes	Cash	Pula	Domestic Pu	Accounting	Retail	1 level - Domestic	6	M	3	M
9	Bagwarash Pesha	Company	C0239589	Bandung, Indonesia	04/08/2009	Indonesia	Maun	Yes	Yes	Yes	EFT	Foreign	Domestic Pri	Legal	Mining	1 level - Foreign	12	H	5	H
9	Mohamed Abaraq	Trust	AG871235	Abbottabad, Afghanistan	03/05/2018	Afghanistan	Francistown	No	Yes	Yes	Card	Virtual	Foreign Publi	NBC related	Tourism	2+ levels - Domestic	20	H	6	H
9	Kelebile Seneo	Individual	849218391	Serowe, Botswana	03/08/1982	Botswana	Serowe	Yes	No	No	Debit Order	Pula	Foreign Publi	other	Public	2+ levels - Foreign	4	L	2	L
													None		Other	Not Determined				
																N/A				
																	Inherent Risk Score	12	H	4	L

Figure. 6 - A sample of a complete risk assessment results.