# EFIU LEGAL PROFESSIONALS

# AML/ CFT GUIDELINE


**March 2024**

# Contents

## ACRONYMS

| | |
|---|---|
| **AML/CFT** | Anti-money Laundering/ Countering the Financing of Terrorism |
| **AML/CFT/PF** | Anti-money Laundering and Combating Financing Terrorism and Proliferation Financing |
| **CDD** | Customer Due Diligence |
| **CRMP** | Compliance Risk Management Program |
| **CTR** | Cash Transaction Report |
| **DNFBP** | Designated Non-Financial Businesses and Professions |
| **EDD** | Enhanced Due Diligence |
| **EFIU** | Eswatini Financial Intelligence Unit |
| **FATF** | Financial Action Task Force |
| **FSRB** | FATF Style Regional Body |
| **INR**. | Interpretive Note to Recommendation |
| **KYC** | Know Your Customer |
| **ML** | Money laundering |
| **MLFTP** | Money Laundering and Financing of Terrorism (Prevention) Act, 2011 as amended. |
| **PEP** | Politically Exposed Person |
| **PF** | Proliferation Financing |
| **RBA** | Risk-based Approach |
| **SRB** | Self-regulatory Body |
| **STR** | Suspicious Transaction Report |
| **TF** | Terrorist Financing |
| **TCSP** | Trusts and company service providers |
| **TPR** | Terrorist Property Reporting |
| **UNSCR** | United Nations Security Council Resolution |

# 1. SECTION 1: INTRODUCTION AND KEY CONCEPT

This Guideline is issued in terms of Section 18bis of the MLFTP, 2011 (as amended). Section 6 of the MLFTP (amendment) Act, 2016 requires that a Legal Professional include the application of a risk-based approach to the management of financial crime risk. The risk-based approach requires that anti-money laundering (AML) and the combatting of the financing of terrorism (CFT) requirements, systems, controls, and preventative measures adopted are commensurate to the risks that are being managed. By applying enhanced measures and controls where the financial crime risks are higher, with the option of applying simplified measures where the risks are lower, Legal Professionals will be able to target their resources more effectively, whilst ensuring that these risks are efficiently mitigated. Legal Professionals shall be required to prepare and submit periodically AML/CFT specific risk assessments to the EFIU at least annually or as and when directed.

The application of a risk-based approach also affords a Legal Professional flexibility to use a range of mechanisms to establish and verify the identities of their clients, creating opportunities to explore more innovative ways of offering services to a broader range of clients and bringing previously excluded sectors of society into the formal economy. This improves the efficacy of measures to combat money laundering and terrorist financing by deploying limited resources to high-risk areas.

The application of a risk-based approach, as also provided for in Recommendation 1 of the Financial Action Task Force (FATF) and section 6 of the Money Laundering and Financing of Terrorism (Prevention) Act, 2011, requires Legal Professional to clearly identify, assess and understand and mitigate the financial crime risks that affect their business. Risk in this context refers to the possible threats and vulnerabilities that could lead to Legal Professional's systems, processes or other elements of the business being abused for purposes of ML/FT/PF, specifically including the facilitation of money laundering, terrorism financing, weapons proliferation, and international sanctions circumvention. By understanding the scope and nature of these risks (through risk profiling and risk assessments), Legal Professional can make informed decisions as to the appropriate methods and controls that should be applied in any given circumstance.

Financial crime risk must be assessed on a holistic basis and by means of a systematic approach. This guideline sets out such an approach, together with the risk framework and minimum requirements that Legal Professional should apply when assessing financial crime risk.

Although the risk-based approach aims to manage financial crime risks more efficiently and effectively, it is not possible to eliminate all financial crime risks. It is Important to note that the risk-based approach does not exempt Legal Professional from mitigating financial crime risks where these risks have been assessed as low.

Furthermore, assessing and mitigating the risk of financial crime is not a static exercise. The risks that have been identified may change or evolve over time as new products or new threats enter the business context.

## 1.1. Purpose of the guideline

The purpose of this guideline is to provide minimum criteria for the application of a risk-based approach by Legal Professional to assist the business in proactively managing financial crime risk by providing for the consistent design, application, and implementation of a risk-based approach. This will further

allow for the optimization of resources to ensure that the allocation of such resources is commensurate with the level of risk identified.

### 1.2. Scope of the guideline

The guideline applies to all Legal practitioners.

### 1.3. Ownership and review of guideline

This guideline is owned by the EFIU and shall be reviewed as and when the need arises and especially informed by legislation or industry practices.

### 1.4. Publication and effective date of guideline

This guidance shall be made available on the EFIU official website on the day of its effective date.

### 1.5. Risk management concepts

The application of a risk-based approach is based on the following concepts:

#### 1.5.1. Risk

Risk can be described as the likelihood and impact of uncertain events on set objectives. The likelihood and impact of such events should be analysed in terms of threats and vulnerabilities.

A threat is a person or group of people, object, or activity with the potential to cause harm. In the context of money laundering and terrorist financing this includes criminals, terrorist groups and their facilitators, their funds, as well as any past, present, and future money laundering, or terrorist financing activities.

The concept of vulnerabilities comprises those things that can be exploited by the threat or that may support or facilitate its activities. Identifying vulnerabilities, as distinct from threats, means focusing on, for example, the factors that represent weaknesses or features that may be exploited in any given system, institution, product, service, etc.

Consequences refers to the impact of a threat or the exploitation of a vulnerability if this impact is to materialize.

Risk in the context of money laundering and terrorist financing therefore refers to the likelihood and impact of money laundering or terrorist financing activities that could materialize because of a combination of threats and vulnerabilities manifesting in the business, or that may jeopardize the detection, investigation or prosecution of these activities or the possibility of the forfeiture of proceeds of unlawful activities.

To have a robust financial crime risk management system, all Legal Professional must be able to demonstrate how they contextualize the concept of “financial crime risk” within their businesses as having an impact on their operational, line management and strategic objectives.

#### 1.5.2. Inherent Risk and Residual Risk

Inherent risk is the risk of an event or circumstance that exists before controls or mitigation measures are applied. Residual risk is the level of risk that remains after controls and mitigation measures have been implemented.

#### 1.5.3. Risk Management

Financial crime risk management is a process that includes the identification of financial crime risks, the assessment of these risks, and the development of methods and controls to manage and mitigate the risks that have been identified.

Financial crime risk, as with other risks, can be managed and mitigated either by avoiding, transferring, tolerating, or treating different risks. Treating financial crime risk entails that the various franchises, segments, subsidiaries, and international operations must develop systems and controls to manage the risks identified. These systems and controls should comprise of all the risk mitigation measures at the business' disposal and should relate to the nature of risks. Such mechanisms include, *inter alia*:

i. the application of client due diligence measures;
ii. the monitoring of business relationships with clients;
iii. managing delivery channels for products and services;
iv. geographic factors
v. structuring the features of products and services; etc.

The process to manage financial crime risk is a continuous cycle. Legal practitioners should be satisfied that the financial crime risk management systems and controls remain adequate in view of changing circumstances relating to emerging threats and vulnerabilities, product innovations, new target markets, changes in circumstances of individual clients or classes of clients, changes in business strategy, etc. This means that financial crime risks, controls and the levels of residual risk must be reassessed at regular intervals. The financial crime risk management systems and controls must also be always adhered to.

### 1.6. Legal Professionals activities and vulnerabilities for ML/TF

It is important to bear in mind when considering the range of tasks undertaken by legal professionals that only specified activities under R.22 must be subject to the AML/CFT regime. The specifics of the risk-based processes of an individual legal professional and/or a firm of legal professionals should accordingly be determined based on the activities undertaken by the legal professional, the ethical and existing supervisory structure for legal professionals and the susceptibility or vulnerability of activities of a legal professional to ML/TF. Mitigating practices will invariably include initial CDD and ongoing monitoring, as well as a range of internal policies, training, and systems to address the vulnerabilities faced in the practice setting of the legal professional.

The basic intent behind the FATF Recommendations is consistent with the role of legal professionals, as guardians of justice and the rule of law, and professionals subject to ethical obligations, namely, to avoid knowingly assisting criminals or facilitating criminal activity. Some of the underlying ethical principles that the legal profession upholds, namely, to avoid facilitating criminal activity and being unwittingly involved in the pursuit of criminal activity, supports the role that legal professionals need to play in the fight against ML/TF.

#### 1.6.1. Client funds

Most legal professionals can hold funds of clients. Client accounts are accounts held by legal professionals with a financial institution. In some civil law countries, a professional body holds the funds of clients, rather than legal professionals. Operating client accounts (trust accounts) require a legal professional to observe AML/CFT obligations. In Eswatini as in most countries, legal professionals are required to hold client funds in a separate account with a financial institution and use the funds only in accordance with their client's instructions. In countries where client accounts are used, legal professionals are required to hold client funds separate from their own. The purpose of these accounts is to hold client funds in "trust" for or for a purpose designated by the client. Funds will also be held or received for payment of costs incurred by the legal professional on behalf of the client. No

funds may pass through a client account without being attached to an underlying legal transaction or purpose, and the legal professional is required to account for these funds. The use of client accounts has been identified as a potential vulnerability, as it may be perceived by criminals as a means to either integrate tainted funds within the mainstream financial system or a means by which tainted funds may be layered in such a way to obscure their source, with fewer questions being asked by financial institutions because of the perceived respectability and legitimacy added by the involvement of the legal professional. Legal professionals can seek to limit their exposure to this risk by developing and implementing policies on the handling of funds (e.g., currency value limits) as well as restricting access to account details to prevent unsanctioned deposits.

### 1.6.2. Advising on the purchase and sale of real property

Real estate, both commercial and residential, accounts for a high proportion of confiscated criminal assets, demonstrating that this as a clear area of vulnerability. In many countries, legal professionals are either required by law to undertake the transfer of property or their involvement is a matter of tradition, custom or practice. However, the specific role of legal professionals in real estate transactions varies significantly from country to country, or even within countries. In some countries, legal professionals will customarily hold or control (e.g., through a financial institution) and transfer or control the transfer of the relevant funds for the purchase of the real estate assets. In other countries this will be done by other parties, such as a title insurance company or escrow agent. In Eswatini this is done by a conveyancer. Even if legal professionals are not handling the funds, they will typically be aware of the financial details and in many cases will be able to inquire about the transaction where appropriate.

Some criminals may seek to invest the proceeds of their crime in real estate without attempting to obscure their ownership of the real estate. Alternatively, criminals may seek to obscure the ownership of real property by using false identities or title the property in the names of family members, friends or business associates, or purchase property through an entity or a trust. Legal professionals will need to consider carefully who they are acting for at the outset of a real estate transaction, especially where there are multiple parties involved in a transaction. In some cases, legal professionals may also opt to apply specific checks on the settlement destinations of transactions (i.e., performing limited CDD on the seller of real property, when acting for the buyer).

### 1.6.3. Formation of companies and trusts

In some countries, legal professionals (in civil law jurisdictions this will usually be a notary) must be involved in the creation of a company. Contrary to our jurisdiction, all lawyers can be involved in the creation of a company. Moreover, members of the public can register a company themselves directly with the registrar of companies, in which case a legal professional's advice is sometimes sought at least in relation to initial liability management, corporate, tax and administrative matters. Criminals may seek the opportunity to retain control over criminally derived assets while frustrating the ability of law enforcement to trace the origin and ownership of the assets. Companies and often trust and other similar legal arrangements are seen by criminals as potentially useful vehicles to achieve this outcome. While shell companies, which do not have any ongoing business activities or assets, may be used for legitimate purposes such as serving as a transaction vehicle, they may also be used to conceal beneficial ownership, or enhance the perception of legitimacy.

Criminals may also seek to misuse shelf companies formed by legal professionals by seeking access to companies that have been 'sitting on the shelf' for a long time. This may be to create the impression that the company is reputable and trading in the ordinary course because it has been in existence for many years. Shelf companies can also add to the overall complexity of entity structures, further concealing the underlying beneficial ownership information.

### 1.6.4. Management of companies and trusts

In some cases, criminals will seek to have legal professionals involved in the management of companies and trusts to provide greater respectability and legitimacy to the company or trust and its activities. In some countries professional rules preclude a legal professional from acting as a trustee or as a company director or require a disclosure of directorship positions to ensure independence and transparency is maintained. In countries where this is permitted, there are diverse rules as to whether that legal professional can also provide external legal advice or otherwise act for the company or trust. This will determine whether any funds relating to activities by the company or trust can go through the relevant legal professional's client account. In addition, in some countries, the non-legal counsel of a legal professional acting in a business capacity may not be protected by the legal professional privilege.

### 1.6.5. Acting as nominee

Individuals may sometimes have legal professionals or other persons hold their shares as a nominee, where there are legitimate privacy, safety, or commercial concerns. However, criminals may also use nominee shareholders to obscure their ownership of assets. In some countries, legal professionals are not permitted to hold shares in entities for whom they provide advice, while in other countries legal professionals regularly act as nominees. Legal professionals should identify beneficial owners when establishing business relations in these situations. This is important to prevent the unlawful use of legal persons and arrangements, by gaining a sufficient understanding of the client to be able to properly assess and mitigate the potential ML/TF risks associated with the business relationship. Where legal professionals are asked to act as nominees, they should understand the reason for this request and ensure that they are able to verify the identity of the beneficial owner of the shares and that the purpose is legitimate.

## 2. SECTION 2: AML/CFT/PF RISK BASED APPROACH

### 2.1 The guiding principles to risk based approach

Legal professionals should base their own risk-based assessments and supporting operating standards and procedures on the following guiding principles:

**2.1.1.** It is advised that legal professionals adopt and demonstrate a zero tolerance for wilful and deliberate non-compliance with AML legislation and regulations.

**2.1.2.** When applying a risk-based approach, legal professionals must comply with all minimum regulatory requirements and all applicable financial crime policies and standards and directives adopted and approved by their boards.

**2.1.3.** Consequences for non-adherence with minimum regulatory and policy requirements should be clearly articulated, specifically for staff members.

**2.1.4.** Each legal professional's Financial Crime Risk Management and Compliance Program will comprise of a collection of documents. These various documents should, as far as possible, provide sufficient guidance on a practical level to its targeted audiences.

**2.1.5.** These documents should, where relevant and appropriate, be read in conjunction with any applicable market conduct standards or guidance.

**2.1.6.** Where applicable, definitions should be agreed and applied consistently across the legal professional. .

**2.1.7.** The design of a risk-based approach must be geared towards truly understanding clients and the risk that they represent, supported by robust client due diligence standards and procedures, and must not simply constitute a tick-box exercise.

**2.1.8.** The risk-based approach adopted by the legal profession should, as far as possible, be designed to be client friendly and not unnecessarily burden the client.

**2.1.9.** The application of a risk-based approach should support the development and strengthening of a culture of compliance in the legal professional's business.

**2.1.10.** The application of a risk-based approach should improve the business' ability to make risk-based decisions.

**2.1.11.** The risk-based approach should enable the use of innovative and cost-effective controls and measures, including the use of new technologies where this is appropriate and effective in managing risk.

**2.1.12.** The risk-based approach should facilitate synergies across franchises, segments, and business units where this is possible and efficient.

**2.1.13.** The risk assessments and franchise risk-based approach documentation must be periodically re-evaluated and updated for it to remain appropriate and current to the risks faced by the business.

### 2.2 Risk management

Risk management framework is a process used to identify the potential threats to an organization and to define the policies and procedures to eliminate or minimize the threats as well as develop a strategy or guideline to monitor and review those identified risk.

An effective financial crime control framework/program requires that the legal professional's business clearly articulate, document, and enforce the way it manages its ML/TF risk. This includes setting specific minimum and maximum levels of risk that must be applied when determining whether a risk can be accepted or not. Some of the questions that the legal professional may want to answer are:

**2.2.1.** Is the business willing to accept regulatory, reputation, legal or financial risks?
**2.2.2.** What risks is the business willing to accept only after implementing some mitigation measures?
**2.2.3.** What risks is the business not willing to accept?

Accepting risk always requires the application of robust governance procedures, which must include escalation of the risk acceptance for approval to the appropriate governance bodies, which must be at an executive committee level.

### 2.3 ML/TF/PF risk assessment and risk rating framework

**2.3.1.** A risk-based approach to AML/CFT means that measures taken to reduce ML/TF are proportionate to the risks. Supervisors and SRBs should have a clear understanding of the ML/TF risks present in their own jurisdiction, as well as improve supervisory effectiveness by allocating resources to areas of higher ML/TF risk, in line with the applicable legal framework and the RBA.

**2.3.2.** Importantly the legal professional's business must include the way it identifies, assesses, mitigates, and manages the ML/TF/PF risk, this includes the ML/TF/PF risk assessment and risk rating methodology in its CRMP document. The legal professional must express and include the inherent ML/TF/PF risk understanding flowing from the ML/TF/PF risk and the risk mitigation, monitoring, and management measures in the CRMP document.

**2.3.3.** This risk-based approach must provide for:

i. A business level risk assessment indicating the ML/TF/PF risk each of the legal professional's different business areas faces.
ii. The way the legal professional's business assesses new products and processes, developed to determine the ML/TF/PF risk ratings or weightings.
iii. A client level risk assessment indicating the ML/TF/PF risk different types of clients pose.
iv. Some of the indicators which broadly includes client type, delivery channel, geographic location, products, and services as well as any other relevant factors.
v. The legal professional must stipulate which indicators should be considered when conducting the risk assessments. The legal professional is cautioned to consider the holistic indicators.
vi. The legal professional must provide evidence that it has conducted client level risk assessments before establishing a business relationship or concluding single transactions with each client.
vii. The legal professional must provide evidence of a business level risk assessment, as well as new products and processes assessment.
viii. A risk matrix could serve as a tool to provide an objective basis to the assessment of several risk indicators because the legal professional's business risk rates/weights the various indicators characteristics and the method of determining the overall risk ratings/weightings. The method may be either a manual or automated manner of calculating ML/TF/PF risk ratings.
ix. The risk-based approach framework should set out the intervals at which the risk rating will be determined including at the establishment of a new business relationship, before conducting a single transaction and thereafter at predetermined ongoing due diligence intervals.
x. The actual risk rating or weighting assigned to each factor's characteristic should be recorded as part of the methodology and applied uniformly when risk rating.
xi. The way to record the outcome/results of the risk assessments that are conducted. (e.g., when a client establishes a business relationship the outcome risk rating is recorded on the client file).

xii. Legal professionals can take an informed decision as to the appropriate methods and levels of verification and enhanced controls that must be applied in each circumstance based on risk assessment results.

xiii. The monitoring, mitigating and management controls that must be applied to the different risk ratings must be clearly noted. The steps that must be taken after having assessed the risk must be indicated.

xiv. The CRMP document must provide for the documenting of decisions taken when dealing with the different levels of ML/TF/PF risk that result.

xv. The Legal Professionals should conduct ML/FT/PF risk assessments and share with the EFIU at least annually.

**2.4 Application of the risk-based approach**

The application of a risk-based approach consists of the following distinct steps:

**2.5 Identification and assessment of inherent risks**

In terms of the new section 6 above, accountable institutions must complete regular financial crime risk assessments. Through these assessments, Legal Professional should identify the financial crime risks they may face in the context of their business and analyse these with a view to understand the likelihood of the risk materializing and the impact that this would have.

The mechanisms used by the legal professional's businesses to identify and assess their financial crime risks must be proportionate to their size and complexity. The risk assessment process therefore might be quite simple or very sophisticated depending on the size and structure of the business and the nature and range of products and services it offers. These risk assessments must form the basis of the risk-based approach that is adopted by the legal professional's business.

Factors that may be indicative of financial crime risks relate to several aspects, including:

i. product offered,
ii. service features associated to products or as stand-alone service,
iii. delivery channels,
iv. geographic areas; and
v. the client risk profile of the business' client base.

Each of these may interact differently with the characteristics of different types of clients.

The examples of factors that may be indicative of financial crime risk provided in **Annexure 1** are not an exhaustive list and legal professionals must therefore also consider other factors that may be relevant to their own businesses. Furthermore, the examples provided here are phrased in neutral terms – i.e., a factor may be indicative of either higher or lower risk depending on the context within which it is considered. It is important therefore to demonstrate how different indicators are brought to bear on a given scenario to reach an appropriate risk classification.

A business risk assessment could utilize a combination of internal subject matter experts; the business risk function; available publications; and external advice. It could also incorporate any future initiatives, previously reported financial crime incidents or events, issues and control failures identified by the respective assurance functions. The assessment must be dynamic and responsive to current and emerging risks.

To be effective, the risk assessment must be properly documented, maintained, and communicated to relevant personnel within the business. A detailed and well documented compliance regime shows commitment to prevent, detect and address non-compliance within the business.

### 2.6 Creating risk- reduction measures and controls

Risk mitigation in the context of financial crime refers to the activities and methods used by the legal professional's business to control and minimize the inherent financial crime risks it has identified. The legal professional's business should therefore apply its knowledge and understanding of its financial crime risks, as assessed per the guidance above, in the development of control measures to mitigate the risks identified. The risk assessment process will therefore assist the legal professional's business in determining the nature and extent of resources necessary to mitigate identified risks.

Each business unit or segment of the legal professional's business must establish and implement systems and controls in response to the assessed risks. These controls must be designed to detect money laundering and terrorist financing and respond appropriately when risks materialize. Where the risks are higher, enhanced measures must be taken to mitigate those risks. This means that the range, degree, frequency or intensity of preventive measures and controls conducted will be stronger in higher risk scenarios. Where the risks have been assessed as lower, simplified measures may be permitted, such as that the degree, frequency and/or the intensity of the controls conducted may be relatively lighter. Legal professionals should always have grounds on which they can base their justification for a decision that the appropriate balance was struck in any given circumstance.

The following are some measures that may be applied in cases of higher risk:

i. Increased automated transaction monitoring,
ii. increased intensity of CDD measures,
iii. increased review periods of client information,
iv. utilizing more or higher quality sources for the vetting of information (impacts both quality and quantity),
v. senior management involvement in decisions to on-board clients,
vi. dedicated specialist staff managing enhanced due diligence for specific clients; and
vii. limited reliance on another accountable institution's controls, together with additional controls.

It is important to note that the risk-based approach requires the business segments of the legal practitioner to adopt effective AML/CFT controls that are commensurate to their assessed risks. It is the responsibility of the business unit to effectively manage all financial crime risks and to meet all applicable minimum legal requirements as the first line of defense.

The systems and controls by which the business decides to manage financial crime risks must be documented in the applicable and relevant accountable institution's processes and procedures.

### 2.7 Assessing residual risks

Residual risk is the risk remaining after taking into consideration the impact and effectiveness of risk mitigation measures and controls. It is important to note that no matter how robust the risk mitigation and risk management program is, the business may always have some exposure to residual risk which must be managed. These risks have been reduced but not eliminated and are therefore still risks.

### 2.8 Evaluating residual risk against set risk appetite

Finally, it must be assessed whether the residual risk that has been identified falls within the set risk appetite of the business. Where the level of residual risk falls outside of the scope of acceptable risk, additional controls and measures must be adopted to mitigate the risk further.

### 2.9 Reviewing the risk- based approach

The risk-based approach implemented by the legal professional's business should be subject to periodic review, as required in terms of paragraph 6 above which is to the effect that legal practitioners carrying out the activities under recommendation 22 above are accountable institutions and shall update their risk assessment policies and programs regularly but at least annually considering new markets and introduction of new products and services, to test the effectiveness of the compliance regime. This review includes but is not limited to:

i. applicable policies and procedures
ii. the risk assessment related to financial crime, including the adequacy of controls and other risk mitigation measures; and
iii. the training program used for employees and senior management.

The risks that have been identified will change or evolve over time as new products or new threats enter the business context. Consequently, the adherence and completion of this step is crucial to the implementation of an effective risk-based approach.

**Whose responsibility is it to undertake a risk assessment?**

The Board of Directors is ultimately responsible for risk management within the legal professional. The board of directors and senior management of the legal professionals are expected to formulate and implement an ML/TF/PF risk assessment framework. The risk assessment must be documented and made available for analysis by EFIU. The board of directors should have a clear understanding of ML/FT/PF risks. Information about ML/FT/PF risk assessment should be communicated to the board in a timely, complete, understandable, and accurate manner so that it is equipped to make informed decisions.

It should be noted that, while the Board of a legal professional may delegate the risk assessment process, the ownership of the risks remains with the operational business units, who are responsible for carrying out any actions resulting from the gaps or deficiencies identified by the risk assessment exercise. Hence the contribution required from each party should be clearly outlined. A legal professional should also ensure that timely and appropriate training and guidance is provided to staff members involved in the completion of the risk assessment to ensure that a consistent approach is taken.

### 2.10 Clients risk profiling requirements

#### 2.10.1 Clients risk assessments

A legal professional's business' AML/CFT Program and policy must require that all clients be risk assessed at the time of on-boarding, or as soon as possible thereafter, and for the duration of the client relationship life cycle on an on-going basis. This initial risk rating therefore represents the inherent risk posed by the client (prior to transactional behaviour commencing) and it is important for purposes of *inter alia* applying the appropriate level of due diligence during the on-boarding process.

A client, for purposes of this guideline, is a natural person or corporate vehicle with whom the legal professional's business has established a business relationship as listed under recommendation 22 above. A business relationship is created at the point at which the client is enabled by the business to

transact, deposit, receive funds or accept products or services offered by the legal practitioner's business.

Risk-rating implies assigning different categories to different levels of risk per a risk scale and classifying the financial crime risks pertaining to different relationships or client engagements in terms of the assigned categories.

The on-going risk assessment of clients comprises of at least two types of risk assessments:

### 2.10.2 Initial risk assessment

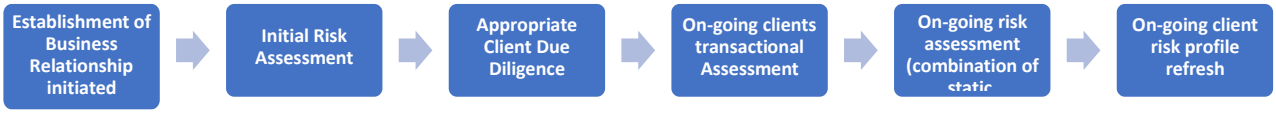
A risk-based approach commences with the assessment of risk that needs to be managed, i.e., the initial risk assessment. This should, where possible, be performed at the time of client on-boarding. Alternatively, the initial risk assessment must be completed as soon as possible once a business relationship has been established.

The initial risk assessment should at a minimum incorporate all relevant and available static client data obtained through the application of the required client due diligence measures.

### 2.10.3 On-going comprehensive risks assessments

While a risk assessment should be performed at the inception of the client relationship, a comprehensive risk profile of the client will only become evident once the client has begun transacting through an account or begins utilizing a service or product. The monitoring of transactions; other client behaviour; and the business relationship are therefore important elements of a well-designed risk-based approach. Once a client has been risk rated, this rating must therefore be continuously re-assessed for the duration of the client relationship life cycle. This risk assessment process flow is illustrated below:

**Figure 1: Risk assessment process flow**




The on-going comprehensive risk assessment models should, in addition to the static factors used for the initial client risk assessment, and to the extent possible, include a dynamic component incorporating the transactional or other behaviour of the client into their risk rating. Once the client starts transacting (where this is applicable), the initial risk assessment may therefore change due to the nature of transactional behaviour of the client or other subsequent factors which may emerge. A lower risk client may thus become higher risk, or alternatively, a higher risk client may become lower risk, based on considerations of both the client static data and transactional behaviour, providing a consolidated and true view of risk of the client relationship. Where possible, this process is to be embedded as an on-going process and not performed as a calendar driven event.

## 2.11 Risk model

Both the initial client risk assessment models and the on-going comprehensive risk assessment models for individuals and entities must be determined by each business segment based on the risk criteria

contained in each legal practitioner's Financial Crime Policy and this guidance, as well as any factors unique to that legal professional's business.

Such models must enable effective and appropriate client risk categorization, considering the money laundering and terrorist financing risk to each legal practitioner's business across its clients; the industries and jurisdictions in which they operate; products offered; delivery channels utilized; and the on-going transactional behaviour of its clients. The ultimate risk rating must be the result of a holistic consideration of these factors.

The following risk factors / variables that, either on their own or in combination, may increase or decrease risk, should be considered when determining the risk rating of a client, unless reasons can be provided showing that a factor is not relevant to a specific risk model in the context of the business in which it will be used:

**Table 1: Inherent Client Risk**

| **Static Variables** | |
|---|---|
| **Inherent Client Risk** | An assessment of the inherent risk of the client, including factors such as the residency status of a client; the nature and frequency of transactions; the legal status of the client (natural person or corporate vehicle) or the legal entity type or structure through which the client operates. Inherent client risk can also include factors such as whether the client has been linked to adverse media relating to financial crime. |

**Table 2: Static Variables**

| **Static Variables** | |
|---|---|
| **Products & services offered** | An assessment of the financial crime risk posed by the products and/or services utilized by the client. It is important to note that criminals constantly alter their methods and techniques and therefore the assessment of products and services must be dynamic. |
| **Geography** | An assessment of the jurisdictions within which the business operates as well as assessment of where clients live and work. |
| **Client industry (Including business activity)** | An assessment of the industry the client works in or, in the case of a business or corporate, the nature of the business. Certain industries are more closely associated with money laundering or terrorist financing risks, as determined by FATF from time to time. Cognizance should also be taken of whether the industry is regulated in the jurisdiction within which it operates. |
| **Distribution channel (which can be assessed as part of product risk)** | The method of distributing products and services at point of account opening as well as on an on-going basis. |

**Table 3: Dynamic Variables**

| **Dynamic Variables** | |
|---|---|
| **Transactional behaviour** | Where applicable, once the client starts transacting, financial crime risk must be assessed based on the client's transactional behaviour. Aggregated transactional risk assessment models for transaction types (e.g., debit card transactions; credit card transactions; electronic funds transfers; and SWIFT |

| | |
|---|---|
| | transactions) may be used to assess client risk in conjunction with the criteria reflected above. |
| **Other behavioral factors** | Where applicable, any other behavioral factors relevant to an assessment of the client's expected behaviour vs. their actual behaviour, and which indicates risk, should be included in the risk model. |

It is imperative that the money laundering risk in any given circumstance be determined on a holistic basis. In other words, the ultimate risk rating accorded to a business relationship or transaction must be a function of all factors that may be relevant to the combination of a client profile, product type and transaction.

The aggregated model should be combined with the initial risk assessment to provide a view of the ongoing risk the client poses to the business. This is illustrated in the diagram below:

**Diagram 4: Risk assessment Diagram**

| **Risk Assessment Diagram** | | | | | |
|---|---|---|---|---|---|
| **Risk Assessment** | **Initial Risk Assessment *(Analytical Modelling)*** | + | **Transactional Risk Assessment *(Analytical Modelling)*** | = | **On-going consolidated Risk Assessment *(Analytical Modelling)*** |
| | ⬇ | | ⬇ | | ⬇ |
| **Controls** | **Level of Client Due Diligence**<br>• **Simplified due diligence.**<br>• **Standard due diligence.**<br>• **Enhanced due diligence.** | | **Transaction Monitoring**<br>• **Suspicious transactions monitoring**<br>• **Cash Threshold monitoring**<br>• **Scenario monitoring**<br>• **Terrorist property monitoring** | | **Client Refresh Cycle**<br>• **Enhanced due diligence (*Annual Refresh)***<br>• **Standard due diligence (*Refresh every 3 years or at trigger event*)**<br>• **Simplified due diligence (*Refresh every 5 years or at trigger event*)** |

The risk-rating methodology and procedures that have been adopted for purposes of client risk rating must be properly documented and are subject to approval by each legal practitioner's board (where applicable). It must furthermore record the basis for allocating risk categories to individual and aggregate risks and the rationale for setting controls against specific risks, including the rationale for the configuration of the financial crime automated systems and risk models.

The factors underlying any given risk-rating will furthermore inevitably change over time. It is therefore essential that the relevance of particular risk factors and the appropriateness of previous risk-ratings be re- assessed on a periodic basis, or when changes to the business, legislative or regulatory environment require such updates.

### 2.12 Automatically high-risk clients

All clients that are deemed to be high risk in accordance with applicable domestic legislation must be risk rated as high, irrespective of any of the other factors in the applicable risk assessment model.

In addition, the following client relationships, when evident, will also result in the overall client relationship becoming high risk, irrespective of any of the other factors in the risk assessment model:

i. Politically Exposed Person as defined in section 2 of the Money Laundering and Financing of Terrorism (Prevention) Act,2011 (MLFTP) 2011 (as amended)
ii. Persons identified as "Persons of Interest" through internal governance structures, and who have been included on the internal business watch lists or exit lists
iii. Money service businesses (MSBs).
iv. Virtual currency providers and exchanges.
v. High commissions and embassies of high-risk jurisdictions, as per the business' Risk Matrix
vi. Foreign charities and foreign trusts.
vii. Arms dealers.
viii. Correspondent banking (Vostro accounts).
ix. Second-hand gold and scrap metal dealers; and
x. Trade, dealing in or breeding endangered or protected species.

The categories of automatically high-risk clients will be reviewed and updated from time to time by each Legal Professional, as the need arises.

Automatically high-risk clients may be reclassified post the completion of EDD. However, where it is a regulatory requirement that a client automatically be deemed to be high risk – as is the case with PEPs. Reclassification is prohibited.

### 2.13 Impact of client risk rating

The client risk rating should inform and determine the processes and controls applicable to that client, or class of clients, which are proportionate to the level of money laundering and terrorism financing risk presented by each client relationship. These processes include, but is not limited to:

i. the appropriate level of client due diligence (CDD) that must be conducted.
ii. the appropriate level of management approval / acceptance required to establish or continue with a business relationship.
iii. the appropriate level of monitoring (transactions and activities); and
iv. the appropriate level and frequency of on-going due diligence (ODD) to be applied.

The processes and controls relating to client due diligence will be set out in further detail in each Legal Professional's Client Due Diligence Minimum Operating Standard.

### 2.14 De-risking

It is important to note that risk assessment does not imply that the legal practitioners' business should seek to avoid risk entirely (also referred to as de-risking), for example, through wholesale termination of client relationships for certain sectors. De-risking poses a threat to financial integrity in general and to the risk-based approach specifically, as it creates opacity in the affected persons' or entities' financial conduct, and it eliminates the possibility to treat financial crime risks. Wholesale refusal of services or termination of services to a class of clients may further give rise to financial exclusion risk and consequently also reputation risk to Legal Professional.

The wholesale termination or restriction of business relationships should therefore, where possible, be avoided as this is an example of inadequate risk management.

### 2.15 Financial crime risk management

i. Legal professionals in their effort to implement an effective Financial Crime Risk Management (FCRM) will develop the client static and transaction risk models as well as the overall risk model which considers both initial and transaction risk as a combined risk.

ii. A legal practitioner's business' (conducting any of the activities under recommendation 22 above) FCRM shall be responsible for documenting the detailed business systems and model configurations and ensuring that these are approved by the Boards or other relevant governance forum. The rationale for the adoption of such system and model configurations, as well as the implementation of the controls must be recorded and monitored by FCRM function of the legal professional's business.

### 2.16 Compliance risk management program (CRMP)

A Legal professional must develop, document, maintain and implement a CRMP for anti-money laundering, combating the financing of terrorism and counter proliferation financing (AML/CTF/CPF), which programme is referred to as the DNFBPs CRMP. The CRMP must provide for all the requirements as set out in the MLFTP Act, UNSCR (2016) and Suppression of Terrorism Act, 2008.

i. Legal professionals must have a main consolidated document or overarching apex document that records the AML/CFT obligations of the accountable institution, which document is referred to as the CRMP.

ii. Legal professionals must express and include the inherent money laundering, terrorist financing and proliferation financing (ML/TF/PF) risk, and its understanding flowing from the ML/TF/PF risk assessments, and the risk mitigation, monitoring as well as the management measures in the CRMP.

# 3. SECTION 3: CUSTOMER DUE DILIGENCE

## 3.1 When to undertake CDD measures:

**3.1.1.** Establishing business relations;

**3.1.2.** There is a suspicion of ML/TF, regardless of any exemptions or thresholds that are referred to elsewhere under the FATF Recommendations; or

**3.1.3.** When a Legal Professional has doubts about the veracity or adequacy of previously obtained customer identification data.

## 3.2 A Legal Professional shall comply with the CDD requirements set out in Section 6 of MLTFP Act 2011, in the following situations:

**3.3.1.** buying and selling of immovable property

**3.3.2.** managing of client money or trust funds, securities, or other assets

**3.3.3.** management of bank, savings, or securities accounts

**3.3.4.** organisation of contributions for the creation, operation, or management of companies;

**3.3.5.** creating, operating or management of legal persons or arrangements, and buying and selling of business entities.

## 3.3 Trust and company service providers –

When a legal professional prepare for or carry out transactions for a client concerning the following activities:

**3.3.1.** Acting as a formation agent of legal persons

**3.3.2.** Acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or similar position in relation to other legal persons.

**3.3.3.** Providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any legal person or arrangement

**3.3.4.** Acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement.

**3.3.5.** acting as (or arranging for another person to act as) a nominee shareholder for another person that have been categorised as Accountable in terms of the MLFTP Act.

## 3.4 Principles of CDD / KYC

A Legal Professional shall abide by the following principles for the effective implementation of their KYC policies.

**3.4.1.** A Legal Professional should know its customers and shall not deal with any person on an anonymous basis, or any person using a fictitious name and should give special attention to the risks arising from new or developing technologies that may favour the anonymity of customers.

**3.4.2.** A Legal Professional shall be required to identify the customer (whether permanent or occasional, and whether a natural or legal person or legal arrangement) and verify that customer's identity using reliable, independent source documents, data, or information (identification data). Provided that, in verifying a natural person's identity, a Legal Professional shall require, among others, the following documents: Full legal names used, including aliases;

**3.4.2.1. Natural Person:**

**i.** National Identity documents (Copy of National ID for Swazi's and Passport for non-Swazis)

ii. Physical address: through Proof of Residence

iii. Sources of Income/wealth
iv. Customer Occupation and Name of Employer (if self-employed, the nature of self-employment)
v. Contact number

**3.4.2.2. Legal Persons and Legal Arrangements:**

i. Name of Company and its Directors: (*National ID for Swazi Directors and Passports for Non-Swazi Directors*)
ii. Company Registered Physical Address
iii. Company Registration Number: (Memorandum and Articles of Associations, Certificate of Incorporation)
iv. Company Contact Person (Name and contact number)

**3.4.2.3. Clubs, Societies and Associations:**

i. Name of Club, Society and Association
ii. Registered address of Club, Society and Association
iii. Company Contact Person (Name and contact number)
iv. By laws or constitutions or rules or regulations of the club or Society or Association. (Certified copies of Club, Society or Association Chairman and signatories)

**3.4.3.** A legal professional shall be required to verify that any person purporting to act on behalf of the customer is so authorised, and identify and verify the identity of that person.

**3.4.4.** A legal Professional shall be required to identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner, using the relevant information or data obtained from a reliable source, such that the Legal Professional is satisfied that it knows who the beneficial owner is.

**3.4.5.** A legal Professional shall be required to inquire if any beneficial owner exists in relation to a customer. Where there is one or more beneficial owners in relation to a customer, a Legal Professional should take reasonable measures to obtain information sufficient to identify and verify the identity of the beneficial owner(s).

**3.4.6.** A legal professional shall understand and, as appropriate, obtain information on, the purpose and intended nature of the business relationship.

**3.4.7.** A legal professional should be required to conduct ongoing due diligence on the business relationship, including:

**3.4.7.1.** Scrutinizing transactions undertaken throughout that relationship to ensure that the transactions being conducted are consistent with the Legal Professional's knowledge of the customer, their business, and risk profile, including where necessary, the source of funds; and;

**3.4.7.2.** Ensuring that documents, data, or information collected under the CDD process is kept up-to-date and relevant by undertaking periodic reviews of existing records, particularly for higher-risk categories of customers.

**3.4.7.3.** A legal profession should pay special attention to all complex or unusually large transactions or unusual patterns of transactions that have no apparent economic or lawful purpose. To the extent possible, the Legal professional should inquire into the background and purpose of all such transactions and document their findings to make this information available to the EFIU should the need arise.

**3.4.8.** For customers that are legal persons or legal arrangements, legal professionals should be required to understand the nature of the customer's business and its ownership and control structure.

**3.4.9.** For customers that are legal persons or legal arrangements, the legal professional should be required to identify the customer and verify its identity through the following information:

**3.4.9.1.** name, legal form and proof of existence;

**3.4.9.2.** the powers that regulate and bind the legal person or arrangement, as well as the names of the relevant persons having a senior management position in the legal person or arrangement; and

**3.4.9.3.** the address of the registered office and, if different, a principal place of business

**3.4.10.** For customers that are legal persons, a legal professional should be required to identify and take reasonable measures to verify the identity of beneficial owners through the following information:

**3.4.10.1.** the identity of the natural person(s) (if any) who ultimately has a controlling ownership interest in a legal person; and

**3.4.10.2.** to the extent that there is doubt under (a) as to whether the person(s) with the controlling ownership interest is the beneficial owner(s) or where no natural person

**3.4.10.3.** exerts control through ownership interests, the identity of the natural person(s) (if any) exercising control of the legal person or arrangement through other means; and

**3.4.10.4.** where no natural person is identified under (a) or (b) above, the identity of the relevant natural person who holds the position of senior managing official

**3.4.11.** For customers that are legal arrangements, a legal professional should be required to identify and take reasonable measures to verify the identity of beneficial owners through the following information:

i. for trusts, the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust (including through a chain of control/ownership);

ii. for other types of legal arrangements, the identity of persons in equivalent or similar positions.

### 3.5 Timing of verification

3.5.1. A legal professional shall verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers; or (if permitted) may complete verification after the establishment of the business relationship, provided that:

i. this occurs as soon as reasonably practicable;

ii. this is essential not to interrupt the normal conduct of business; and

iii. the ML/TF risks are effectively managed

3.5.2. A legal professional shall adopt risk management procedures concerning the conditions under which a customer may utilise the business relationship prior to verification.

### 3.6 Existing Customers

A legal professional shall apply CDD requirements to existing customers on the basis of materiality and risk, and to conduct due diligence on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.

### 3.7 Risk Based Approach

A legal professional shall perform enhanced due diligence where the ML/TF risks are higher.

A legal professional may only be permitted to apply simplified CDD measures where lower risks have been identified, through an adequate analysis of risks by the country or the financial institution. The simplified measures should be commensurate with the lower risk factors, but are not acceptable whenever there is suspicion of ML/TF, or specific higher risk scenarios apply.

### 3.8 Failure to satisfactorily complete CDD:

Where a legal professional is unable to comply with relevant CDD measures:

i. it should be required not to open the account, commence business relations or perform the transaction; or should be required to terminate the business relationship; and
ii. it should be required to consider making a suspicious transaction report (STR) in relation to the customer

### 3.9 CDD and tipping-off

In cases where a legal professional forms a suspicion of money laundering or terrorist financing, and they reasonably believe that performing the CDD process will tip-off the customer, they should be permitted not to pursue the CDD process, and instead should be required to file an STR.

### 3.10 Simplified Customer Due-Diligence

Where the risks of ML/TF are lower, a legal professional is permitted to conduct simplified CDD measures, which should take into account the nature of the lower risk. The option to apply simplified due diligence is not mandatory, it is something a legal professional may elect to do. Simplified due diligence is not an exemption from any of the CDD measures, however it allows legal professional to adjust the amount, timing, or type of each or all of the CDD measures in a way that is commensurate to the low risk identified. Therefore, simplified measures shall be commensurate with the lower risk factors (e.g. the simplified measures could relate only to customer acceptance measures or to aspects of ongoing monitoring).

Examples of possible measures are:

i. Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (e.g. if account transactions rise above a defined monetary threshold).
ii. Reducing the frequency of customer identification updates.
iii. Reducing the degree of on-going monitoring and scrutinising transactions, based on a reasonable monetary threshold.
iv. Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established.

Simplified CDD measures are not acceptable whenever there is a suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply.

### 3.11 Non-face-to-face Verification

i. A legal professional should put in place policies and procedures to address specific risks associated with non-face-to-face business relationships or transactions, which should be implemented when establishing business relations and transacting through instructions conveyed by customers over the post, telephone, or Internet.

ii. Where there is no face-to-face contact, a legal professional should use equally effective identification and verification procedures as those available for face-to-face customer acceptance, supplemented with specific and adequate measures to mitigate the higher risk. It is important to note that not all non-face-to-face business relationships will present higher risk.

### 3.12 Customer exit

Legal professionals must implement procedures and processes to manage the exit of customer relationships where they are prohibited or present an unacceptable financial crime risk. This must include the requirement to:

i. Assess the customer relationship and document.

ii. The financial crime risks posed by the customer with reference to the AML/ CFT risk appetite and any contractual conditions, regulatory expectations and, where applicable, competition law, that must be considered in deciding whether to retain or exit the customer relationship as well as the rationale for the decision to exit the customer relationship.

iii. Specify a plan and timeline for exiting the customer relationship in line with the existing forum established for this purpose.

# 4. SECTION 4: ENHANCED DUE DILIGENCE

## 4.1. When EDD is Required

**4.1.1.** A legal professional is required to apply EDD for such categories of customers, business relationships, or transactions that are determined to present higher ML/TF risk due to business activity, ownership structure, nationality, residence status, politically exposed status, or other higher-risk indicators.

**4.1.2.** A legal professional shall ensure that monitoring systems are appropriately tailored and provide timely and comprehensive reports to facilitate effective monitoring of such relationships and periodic reporting on such relationships to senior management and the Board.

## 4.2. Enhanced Monitoring

The following are examples of measures a legal professional may employ to monitor high-risk customers:

i. Conducting more frequent reviews of the business relationship and establishing more stringent thresholds for updating CDD information;
ii. Setting specific business limits or parameters regarding accounts or transactions that would trigger early warning signals and require mandatory review;
iii. Requiring senior management approval at the transaction level for products and services that are new for the customer;
iv. Reviewing transactions more frequently against red flag indicators relevant to the relationship. This may include establishing the purpose and destination of funds and obtaining more information on the beneficiary before conducting the transaction;
v. Flagging unusual activities and escalating concerns and transactions for senior management's attention.
vi. Ascertain source of funds and source of wealth of the customer and of the customer's beneficial owner

## 4.3. Examples of EDD Measures

Where the risks of money laundering or terrorist financing are higher, a legal professional should be required to conduct enhanced CDD measures, consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious. Examples of enhanced CDD measures that could be applied for higher-risk business relationships include:

i. In any case which legal professional has identified presents a high risk of ML/TF
ii. in any transaction or business relationship with a person established in a high risk jurisdiction.
iii. Where the customer/potential customer is a PEP, or a family member, or a close associate with a PEP.
iv. Where the customer is a foreign PEP
v. Where a customer has provided false or stollen identity documentation or information in any case where :
vi. the matter or transaction is complex or unusually large or there is an unusual pattern of transaction.
vii. transaction have no apparent economic or legal purpose or in any other case by its nature can present high risk of ML/TF.

### 4.4. How to Conduct EDD

**4.4.1.** Obtaining additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of customer and beneficial owner.
**4.4.2.** Obtaining additional information on the intended nature of the business relationship.
**4.4.3.** Obtaining information on the source of funds or source of wealth of the customer.
**4.4.4.** Obtaining information on the reasons for intended or performed transactions.
**4.4.5.** Obtaining the approval of senior management to commence or continue the business relationship.
**4.4.6.** Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.
**4.4.7.** Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

### 4.5. High risk jurisdiction

i. A legal professional shall apply enhanced due diligence measures to business relationships and transactions with natural and legal persons, and financial institution, from countries for which this is called for by the FATF. The type of enhanced due diligence measures applied should be effective and proportionate to the risks.
ii. A legal professional shall consider establishing adequate internal policies, procedures, and controls in relation to the application of EDD measures and risk proportionate effective countermeasures to customers and business relationships associated with high-risk countries commensurate with the nature, size of the business and the risks involved.

### 4.6. EDD measures in high-risk jurisdictions

EDD measures for matters involving high-risk third countries must include:

i. obtaining additional information on the customer and on the customer's beneficial owner. obtaining additional information on the intended nature of the business relationship
ii. ii) obtaining information on the source of funds and source of wealth of the customer and of the customer's beneficial owner
iii. iii) obtaining information on the reasons for the transactions
iv. obtaining the approval of senior management for establishing or continuing the business relationship
v. conducting enhanced monitoring of the business relationship by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination

### 4.7. Politically Exposed Persons (PEP)

A Politically Exposed Persons (PEP) is an individual who is entrusted with prominent public functions, other than as a middle-ranking or more junior official, including:

i. heads of state, heads of government, ministers and deputy or assistant ministers
ii. members of parliament or of similar legislative bodies
iii. members of the governing bodies of political parties
iv. members of supreme courts, of constitutional courts or of any other judicial body the decisions of which are not subject to further appeal except in exceptional circumstances
v. members of courts of auditors or of the boards of central banks
vi. ambassadors, charges d'affaires and high-ranking officers in the armed forces

vii. members of the administrative, management or supervisory bodies of State[1]owned enterprises
viii. directors, deputy directors and members of the board or equivalent function of an international organization

Individuals who have, or have had, a high political profile, or hold, or have held, public office, can pose a higher money laundering risk to organizations as their position may make them vulnerable to corruption. This risk also extends to members of their immediate families and known close associates. Politically exposed person (PEP) status itself does not, of course, incriminate individuals or entities, but it does put the customer or the beneficial owner into a higher risk category.

A legal professional must have in place appropriate risk-management systems and procedures to determine whether a customer or its beneficial owner is (i) a PEP, and/or (ii) a family member or known close associate of a PEP and to manage the enhanced risks arising from institutions' business relationship or transactions with such a customer.

### 4.8. Domestic PEPs

In relation to domestic PEPs or persons who have been entrusted with a prominent function by an international organisation, in addition to performing the CDD measures required under section 6 of the MLTFP Act, a Legal Professional is required to:

i. take reasonable measures to determine whether a customer or the beneficial owner is such a person; and
ii. in cases when there is higher risk business relationship with such a person, legal professional shall:
iii. put in place risk management systems to determine whether a customer or the beneficial owner is a PEP;
iv. obtain senior management approval before establishing (or continuing, for existing customers) such business relationships;
v. take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as PEPs; and
vi. conduct enhanced ongoing monitoring on that relationship.

### 4.9. Foreign PEPS

In relation to foreign PEPs, in addition to performing the CDD measures required under Section 3 of the guideline, legal professionals shall:

i. put in place risk management systems to determine whether a customer or the beneficial owner is a PEP;
ii. obtain senior management approval before establishing (or continuing, for existing customers) such business relationships;
iii. take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as PEPs; and
iv. conduct enhanced ongoing monitoring on that relationship.

Legal Professionals shall apply relevant requirements of domestic and foreign PEPs to family members or close associations of all types of PEP.

### 4.10. How to Identify PEPs

A legal professional shall have in place appropriate risk-management systems and procedures to determine whether a customer or its beneficial owner is a PEP, and/or a family member or known close associate of a PEP and to manage the enhanced risks arising from institutions' business relationship or transactions with such a customer.

A combination of activities may be used to make the PEP determination. For example, a Legal Professional may:

**4.10.1.** periodically monitor their existing client base against changes in the PEP universe and not just at the time of client on-boarding.

**4.10.2.** Outside of periodic screening, a legal professional may also rely on media monitoring to identify PEPs. For example, newspaper announcements regarding changes to board members of state-owned corporations. Additional sources of information include the Government website (foreign or domestic), and Parliament website (foreign or domestic), the EFIU website (foreign or domestic); and the website of the FATF.

**4.10.3.** If the individual customer is a close family member or close associate, the relationship of the person to the PEP must be documented;

**4.10.4.** Understanding and documenting the nature and intended purpose of the relationship/account, the source of the initial funds (where appropriate), and the anticipated levels of account activity;

**4.10.5.** Understanding and documenting the customer's source of funds and source of wealth (e.g. salary and compensation from official duties and wealth derived from other sources). Where the risks are high or there are doubts as to the veracity of the information provided by the customer, A Legal Professional must validate this information using independent and reliable sources;

**4.10.6.** Conduct Negative News or Adverse Media screening on the customer and evaluate any positive hits.

**4.10.7.** during account opening procedures, include a specific question on PEP status and/or capture occupation to identify holders of public office.

### 4.11. Politically exposed persons documentation

Legal professionals must document their processes regarding Politically Exposed Persons in the CRMP document which sets out:

i. The way to scrutinise prospective clients, persons acting on behalf of the client and beneficial owner's information to determine whether they are domestic PEPs, their immediate family members or known close associates.

ii. The way the legal professional will obtain senior management approval to establish a business relationship with a Foreign PEP & local PEP.

iii. The data sources relied upon to determine whether a client is a PEP.

### 4.12. PEP categorization

In terms of this guideline, and in accordance with FATF Recommendation 12, and the Money Laundering and Terrorist Financing (Prevention) Act 2011, as amended, PEPs have been categorized as follows:

**4.12.1.** A Head of State or Government- King, Prime Minister, Deputy Prime Minister, and all cabinet Ministers.

**4.12.2.** A politician on the national level- All members of the house of Senate and House of Assembly, Consular, Ambassadors.

**4.12.3.** A senior Government official: Undersecretary, Private secretary, Chiefs, Tindvuna.

**4.12.4.** Judiciary- The country's judicial members including all Judges and Magistrates.

**4.12.5.** Military Official-Head of Royal Eswatini police, Eswatini Umbutfo Defence Force, His Majesty's Correctional services, Fire, and emergency services.

**4.12.6.** A senior executive of a State-owned enterprise.

**4.12.7.** An individual or undertaking identified as having.

i. close family ties or personal or business connections to any of the persons.

ii. Immediate Family Members due to their proximity to the person entrusted with the prominent public office, the associated PEP may be able to abuse the position of a family member to undertake illicit activities.

**4.12.8.** To this section, an immediate family member includes –

i. the spouse, civil partner, or life partner.
ii. the previous spouse, civil partner, or life partner, if applicable
iii. children and stepchildren and their spouse, adopted children and their adoptive parents, civil partner, or life partner.
iv. parents; and siblings and step siblings and their spouse, civil partner or life partner and known close associates. Known close associates should be similarly categorized and subjected to the same requirements set out in this guideline, as applicable.

The category of "closely associated persons" typically includes close business colleagues and personal advisers / consultants to the PEP, as well as persons who obviously benefit significantly from being close to such a person. Close associates can therefore be individuals who are closely connected to a PEP, either socially or professionally. Due to their proximity to the person entrusted with the prominent public office, the PEP may be able to abuse the position of an associate to undertake illicit activities.

# 5. SECTION 5: AML/CFT INTERNAL CONTROLS

Legal Professionals must adopt appropriate controls regarding the size and the nature of the business. There is no standard solution to the design of internal control systems, and this should be considered when legal professionals are devising an AML/CFT framework. Internal controls will also depend on the business structure, size, and internal organisation without prejudice to the effectiveness of the system. Policies, procedures, and control systems must be designed and implemented with a view to ensuring the ML/TF risks are promptly identified and mitigated in line with the RBA. Internal control systems must be evaluated to determine how effectively they are dealing with the overall risks. Risk-based processes must be established within the internal controls of the businesses to be effective. To be successful, internal policies and procedures are largely dependent on the internal control systems.

## 5.1 The internal controls for Legal Professionals

Legal Professions businesses should include the following internal policies, procedures and controls:

i. compliance management arrangements (including the appointment of a compliance officer at the management level);
ii. screening procedures to ensure high standards when hiring employees;
iii. an ongoing employee training programme; and
iv. an independent audit function to test the system.

## 5.2 Governance

For the AML/CFT/PF framework of a Legal Professional to be effective, it must be based on the foundation of a sound governance structure and held together by a strong compliance culture. This includes appropriate management structures that are accountable for clear ML/TF/PF risk management and mitigation measures, as well as appropriate independent control functions. It is therefore imperative that the board and senior management of a legal professional ensure that the policies, procedures, systems, and processes put in place to prevent ML/FT are appropriate. The AML/CFT/PF program of a Legal Professional must be risk-based and commensurate with the nature, size, complexity, and inherent risks of the legal professional.

### 5.2.1. The Role of the Board

The Board of Directors of a Legal Professional has oversight and accountability for the AML/CFT/PF compliance program and monitoring the effectiveness of the AML/CFT/PF Risk Management and Compliance Program regularly. It is the responsibility of the Board to ensure compliance by a legal professional and its employees with the provisions of the MLTFP Act and the AML/CFT/PF Risk Management and Compliance Program.

Key responsibilities of the Board include:

i. Approving the AML/CFT/PF compliance program including all AML/CFT/PF policies;
ii. Ensuring the establishment of appropriate mechanisms to periodically review key AML/CFT/PF policies to ensure their continued relevance in line with changes in the products and services and to address new and emerging ML/TF/PF risks of a legal professional;
iii. Ensuring the establishment of an appropriate AML/CFT/PF risk management framework with clearly defined lines of authority and responsibility for AML/CFT/PF and effective separation of duties between those implementing the policies and procedures and those enforcing the controls;
iv. Ensuring that the Board receives the requisite training on AML/CFT/PF generally as well as on a legal professional's specific AML/CFT/PF risks and controls;

v. Ensuring receipt of regular and comprehensive management information and reports on the AML/CFT/PF risks from the Compliance Officer and or senior management or board committees of the legal professional.

### 5.2.2. Role of Senior Management

Senior Management is responsible and accountable for the day-to-day implementation and management of the AML/CFT/PF Compliance Program. Senior Management has to ensure that it is adequate to mitigate ML/TF/PF risks and that it is implemented effectively in all relevant business areas, including ensuring adherence to established AML/CFT/PF policies and procedures.

**Senior Management should ensure that:**

i. policies and procedures are risk-based, proportional, and adequate to mitigate ML and TF risks of the Legal Professional;
ii. the Legal Professional complies with all relevant AML/CFT/PF laws, regulations and guidelines;
iii. are implemented effectively across relevant business areas or throughout the financial group as applicable;
iv. review policies and procedures periodically for consistency with the business model, product and service offerings, and risk appetite of the Legal Professional;
v. Senior Management must review policies and procedures periodically for consistency with the business model, product and service offerings, and risk appetite of the Legal Professional. Attention should be paid to new and developing technologies and Legal Professionals should identify and assess the ML/FT/PF risks arising from new products, services and delivery channels; new business practices and new or developing technologies for new and existing products; and put measures in place to manage and mitigate such risks;
vi. Risk assessments take place before the launch or use of such products, services, channels, business practices, and technologies;
vii. All significant recommendations made by internal and external auditors and regulators in respect of the AML/CFT/PF program are acted upon in a timely manner;
viii. Relevant, adequate, and timely information regarding AML/CFT/PF matters is provided to the Board;
ix. There is an ongoing employee training program that enables employees to have sufficient knowledge to understand and discharge their AML/CFT/PF responsibilities.

### 5.2.3. Vetting of Compliance Officer

A legal professional should check that staff have integrity and are adequately skilled and possess the knowledge and expertise necessary to carry out their function, in particular where staff are responsible for implementing AML/CFT controls in line with Section 18 of the MLFTP Act.

The level of vetting procedures of staff should reflect the ML/TF risks to which individual staff are exposed and not focus merely on senior management roles. Steps should be taken to manage potential conflicts of interest for staff with AML/CFT/PF responsibilities

**Appointment and Responsibilities of the Compliance Officer:**

i. For purposes of ensuring compliance with Section 18 of the MLFTP Act, a legal Professional must appoint a Compliance Officer with the appropriate seniority status, relevant qualifications, and experience to perform the statutory duties and responsibilities associated with this role, including keeping abreast of the latest developments in ML/FT/PF techniques and the AML/CFT/PF best practices within the industry. The Compliance Officer must have sufficient

authority, independence, and seniority to be able to effectively carry out his duties in accordance with the MLFTP Act.

ii. This individual is responsible for creating, deploying, and organizing AML systems and controls. In addition, they report to state and federal authorities in the event of suspicious activity or financial crimes. Where a legal professional does not employ more than five (5) employees, the most senior employee shall be the Compliance Officer. The Compliance Officer has the overall responsibility for the implementation of the enterprise-wide AML/CFT/PF compliance program.

iii. The nature of the reporting line of the Compliance Officer – the Compliance Officer should have a direct reporting line to the Board of Directors (or relevant Committee of the Board) of a legal professional. For smaller legal professional settings where independence may not be practical, that legal professional must consider the administrative reporting lines of the Compliance Officer. Ultimately, a legal professional must be able to demonstrate the independence of the Compliance Officer in instances where practically, independence cannot be achieved functionally.

### 5.3 Employee Vetting and Recruitment

Legal professionals should check that staff have integrity and are adequately skilled and posses the knowledge and expertise necessary to carry out their functions.

In addition to knowing the customer, a legal professional must have robust procedures in place for knowing its employees. In this regard, every legal professional should have a know-your-employee or recruitment policy to attract and retain employees of the highest levels of integrity and competence. The ability to implement an effective AML/CFT/PF program depends in part on the quality and integrity of employees.

**5.3.1** A legal professional should undertake due diligence on prospective employees and throughout employment. A legal professional shall, amongst others:

i. Verify the applicant's identity and personal information including employment history and background.

ii. Develop a risk-based approach to determining when pre-employment background screening is considered appropriate or when the level of screening should be increased, based on the position and responsibilities associated with a particular position. The sensitivity of the position or the access level of an individual employee may warrant additional background screening, which should include verification of references, experience, educational, professional qualifications, and financial crime background;

iii. Maintain an ongoing approach to screening for specific positions, as circumstances change, or for a comprehensive review of employees over a period of time. Internal policies and procedures should be in place (e.g., codes for conduct, ethics, conflicts of interest) for assessing employees;

iv. Have a policy that addresses appropriate actions when pre-employment or subsequent due diligence detects information contrary to what the applicant or employee provided;

v. Have a robust recruitment policy: a legal professional should implement ongoing monitoring of employees to ensure that they continue to meet the standards of integrity and competence of the legal professional.

### 5.3.2 Employee Due Diligence Process - Existing Employees

i. If an Employee is offered a promotion or is offered a role which increases their level of responsibility or autonomy, the human resources department must give the employee a description of the role.
ii. Having regard to the legal profession's ML/TF risks, the HRM must assign the proposed role a risk rating, having regard to whether the role would be reasonably likely to allow the person a significant opportunity to facilitate ML or TF activity.
iii. If the HRM assigns a high risk to the role, the HRM must ensure to obtain, to the extent that they have not earlier been obtained in relation to the Employee, the results of the same checks.
iv. If these checks reveal any adverse or seriously inconsistent results, the AML/CFT Compliance Officer and human resources department will consider and make appropriate decision. A record of all searches conducted and any discussions in relation to a decision to employ must be recorded and maintained in accordance with the record keeping obligations.

## 5.4 Training

The effective application of AML/CFT/PF policies and procedures depends on staff's knowledge and understanding of not only the processes they are required to follow but also the risks these processes are designed to mitigate, as well as the possible consequences of those risks. The legal professional must ensure that staff receive AML/CFT/PF training, which should be:

i. of high quality, relevant to the institution's ML/TF risks, business activities and up to date with the latest legal and regulatory obligations, and internal controls;
ii. obligatory for all relevant staff;
iii. tailored to particular lines of business within the institution, equipping staff with a sound understanding of specialized ML/TF/P risks they are likely to face and their obligations in relation to those risks;
iv. effective, which can be checked for example by requiring staff to pass tests or by monitoring levels of compliance with the institution's AML/CFT/P controls and applying appropriate measures where staff are unable to demonstrate the level of knowledge expected;
v. ongoing, regular, relevant, and not be a once-off exercise; and
vi. complemented by AML/CFT/P information and updates that are disseminated to relevant staff as appropriate.

## 5.5 Audit and Assessment of Controls

A legal profession should conduct independent testing on the AML/CFT/PF compliance program. A legal profession should maintain an adequately resourced and independent audit function to test compliance with policies, procedures and controls.

An internal audit system and an independent audit program that will ensure the completeness and accuracy of information obtained from customers. A legal professional shall specify in writing the examination scope of independent audits, which shall include ensuring checking the accuracy and completeness of identification documents, cash transaction report (CTR) and suspicious transaction report (STR) submitted to the EFIU, and records retained in compliance with this framework, as well as assuring adequacy and effectiveness of the legal professional's training programs;

# 6. SECTION 6: TARGETED FINANCIAL SANCTIONS

## 6.1 United Nations Security Council Resolutions

The sanctions review aims to apply Targeted Financial Sanctions (TFS) against all individuals listed by the UN Security Council. A legal professional must screen customers or potential customers involved in transactions against United Nations Security Council Resolution (UNSCR) sanctions lists. Such screening must be performed before opening accounts or before giving a customer access to the services, regardless of whether the customer is dealing below or above the CDD threshold. This is necessary to combat TF and PF activities by ensuring that selected individuals, organizations, or countries are identified and do not benefit from improperly exploited services and that their funds and assets are frozen accordingly. The term "targeted economic sanctions" primarily refers to the immediate freezing of assets and the prohibition of making funds or other property or services directly or indirectly available to sanctioned individuals, entities, or groups.

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

i. The freezing of funds and other financial assets and economic resources, including preventing their use, alteration, movement, transfer, or access; and
ii. The freezing of economic resources also includes preventing their use to obtain funds or other assets or services in any way, including, but not limited to, selling or mortgaging them.
iii. Reporting transaction under this part to the EFIU.

## 6.2 Obligation to report sanctions

A person to whom a designation or sanctions list is submitted, shall where applicable;

i. Take necessary steps to freeze the funds owned or controlled by the designated entity without delay and without notice to the entity;
ii. Within twenty-four hours of detecting the funds and freezing the funds, file a suspicious transaction report with EFIU in such form as may be required under Section 12 of the MLFTP Act.
iii. Take such other action as may be necessary to give effect to resolution 1267, 1373, 1718 and 1988 and other related resolutions.

## 6.3 Sanction Screening

i. A Legal Professional must be able to determine whether they have a sanctioned person or entity as a client or whether a prospective client is a sanctioned person or entity to determine their exposure to TFS-related obligations. This implies that a legal professional which is likely to encounter sanctioned persons or entities can screen clients and prospective clients against the relevant sanctions lists. This should be done during the client-take-on process as well as subsequently as and when the UNSC adopts new TFS measures or expand existing ones.
ii. A Legal Professional must therefore determine the likelihood that their client base and intended target market may include sanctioned persons or entities. This should assist the Legal Professional in determining the amount of effort and resources it requires to determine whether they have sanctioned persons or entities as a client or whether prospective clients are sanctioned persons or entities. A Legal Professional that has business relationships with foreign persons and entities are more vulnerable to dealing with sanctioned persons and entities.

### 6.4 Mechanism for implementation

Mechanisms for the implementation of the UNSC Resolutions include the circulation of the Designation or List by the United Nations Security Council Resolutions Implementation Committee to the EFIU, other supervisory authority, REPS, such other law enforcement agencies.

The EFIU or a supervisory body shall, upon receipt of the designations or sanctions list submitted to it under sub-regulation (4);

i. Circulate the designations or sanction list to reporting entities under its purview for their information and action;
ii. Where necessary, provide guidance to reporting institutions holding funds or other assets of a designated person, in relation to their obligations under UNSC Regulations and
iii. Ensure that the reporting institutions comply with the requirements of these UNSC Regulations

### 6.5 Targeted financial sanctions controls relating to terrorist financing.

**6.5.1.** A Legal Professional must detail the process to comply with the targeted financial sanctions regime aimed at terrorist financing in the CRMP document.

**6.5.2. A targeted financial sanctions process must provide for:**

i. The way A Legal Professional will scrutinize client information to identify persons listed on a United Nations Security Council 1267 resolutions list, OFAC, EU
ii. The systems used and supporting processes for scrutinizing client information.
iii. The freezing of accounts process that must be followed should a client or potential client be listed on a TF list.
iv. It is important to note that client information includes information regarding the client, prospective client, beneficial owner, person acting on behalf of the client and transaction/payment information.

### 6.6 Targeted financial sanctions controls relating to proliferation financing.

**6.6.1.** A Legal Professional must document its process in place to comply with the targeted financial sanctions regime aimed at proliferation financing in the CRMP document.

**6.6.2.** A targeted financial sanctions process must provide for:

i. The way the legal professional's business will scrutinize client information to identify persons listed on a TF list as published in terms of UNSC Regulations.
ii. The systems used and supporting processes for scrutinize client information.
iii. The freezing process that must be followed should a client or potential client be listed on a sanction list.
iv. It is important to note that client information includes information regarding the client, prospective client, beneficial owner, person acting on behalf of the client and transaction/payment information.

### 6.7 Importance of an effective freezing regime

Effective freezing regimes are critical to combating the financing of terrorism and, as a preventive tool, accomplish much more than freezing terrorist-related funds or other assets present at any time. Effective freezing regimes also combat terrorism by:

i. Deterring non-designated persons or entities who might otherwise be willing to finance terrorist activity.
ii. Exposing terrorist financing "money trails" that may generate leads to previously unknown terrorist cells and financiers.

iii. Dismantling terrorist financing networks by encouraging designated persons or entities to disassociate themselves from terrorist activity and renounce their affiliation with terrorist groups.
iv. Terminating terrorist cash flows by shutting down the pipelines used to move terrorist.
v. related funds or other assets.

### 6.8 Identifying information

i. For the effective implementation of an asset freeze, robust identifying information is essential. At the extreme end of the scale, poor quality identifiers are an obstacle to the enforcement of an asset freeze. Single name identifiers represent problems for enforcement.
ii. Best efforts should therefore be made to ensure as much identifying information as possible is provided upon designation, and that such information be updated as more identifying data become available.

## 7. SECTION 7: RECORD KEEPING

### 7.1 Obligation to keep records

A Legal Professional are to adopt appropriate record keeping guidelines in accordance with Section 8 of MLFTP (Amendment) Act. The nature and size of the business will determine the type of documents to be kept, and the method that will be used . The system used to retain the documents should be eligible enough to allow the company to be able to reconstruct records in the event a supervisory authority requests the legal professional's business to do so. The customer records to be kept should be relevant to the customer's profile. A legal professional shall maintain all necessary records on transactions, both domestic and international, for at least five years following completion of the transaction.

### 7.2 Obligation to keep CDD and transactions records

i. A legal professional shall keep all records obtained through CDD measures, account files and business correspondence, and results of any analysis undertaken, for at least five years following the termination of the business relationship or after the date of the occasional transaction.
ii. Transaction records should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity.
iii. A legal professional shall ensure that all CDD information and transaction records are available swiftly to domestic competent authorities upon appropriate authority.

### 7.3 Obligation to keep STR and CTR records

i. A legal professional shall maintain records concerning its internal reporting of STR and CTR, and decision making whether to file or not to file said reports, for atleast a period of five (5) years from the date of submission.

### 7.4 Manner in which records must be kept

i. A legal professional shall also maintain and safely store for atleast five (5) from the dates the contractual relationship was terminated, all records of customer identification and transaction documents.
ii. A legal professional shall like-wise keep electronic copies of all covered STR and CTR records or reports for atleast five years from the date of filing.
iii. A legal professional should put in place a documented record keeping and reporting policy that provides for maintenance of variety of records.

### 7.5 Reliance on third parties

A legal Professional may use the services of a third party for collecting and the performance of CDD measures, keeping and maintaining of records as long as the records can be obtained upon request and without delay by internal, and external auditors, law and that the third party adheres to the record-keeping provisions of Section 8 bis of MLFTP (Amendment) Act.

i. In addition a legal professional shall satisfy itself that it has measures in place for compliance with record keeping requirements in line with section 8 bis of the MLFTP (Amendment)
ii. The records must be kept in a manner that will ensure that they are safe from any hazards as such as water, fire or pest that may deface them.
iii. A legal professional should keep records in a secure manor and ensure that access to this facility is managed or controlled. It is important that the access and movement of a document is monitored or controlled within the organization to ensure that documents taken from files are returned and are not lost.

# 8. SECTION 8: SUSPICIOUS TRANSACTIONS REPORTING

## 8.1 Obligation to report an STR

i. A legal professional must report suspicious transactions, attempted suspicious transactions, and where there are reasonable grounds to suspect that a transaction may be related to the commission of a criminal activity or related to ML/TF/PF. A legal professional must provide any additional information required by the EFIU in relation to the filed suspicious transaction reports.

ii. All suspicious or unusual transactions must be reported to the EFIU within two (2) days of forming the suspicion regardless of the amount of transaction or funds involved.

iii. To fulfil the reporting obligation, a Legal professional must have a policy that will establish procedures for statutory obligations on suspicious activity reporting to the EFIU. These procedures should also reflect the principle of confidentiality, ensure that investigation is conducted swiftly and that reports contain relevant information and are produced and submitted in a timely manner. The Compliance Officer must ensure prompt disclosures where funds or other property that is suspected to be the proceeds of crime remain in an account.

## 8.2 Identification, investigation, and reporting of suspicious transactions

i. A legal professional shall implement adequate internal policies, procedures and controls in relation to identification and reporting of suspicious transactions to the EFIU. These should be communicated to all staff members of the legal professional.

ii. Where a Legal Professional suspect, or has reasonable grounds to suspect, that funds are the proceeds of crime or are related to terrorist financing, it shall report its suspicions not later than 2 working days to the EFIU. A Legal Professional should have the ability to flag unusual movement of funds or transactions for further analysis.

iii. Further, a Legal Professional should have appropriate case management systems so that such funds or transactions are scrutinized in a timely manner to whether the funds or transaction are suspicious.

iv. To fulfil this obligation, a legal professional must also put in place and update indicators that can be used to identify the suspicion of criminal activity and involvement in ML/TF/PF activities. Examples of suspicious activities are set out in Annexure 1 of the guideline.

## 8.3 Tipping-off and Confidentiality

**8.3.1** A Legal Professional, directors, officers, employees, and auditors of the Legal professional are:

i. prohibited from disclosing ("tipping-off") the fact that a suspicious transaction report (STR) or related information is being filed with the EFIU; and

ii. protected from civil, criminal, or disciplinary proceedings if they report their suspicions in good faith to the EFIU, even if they did not know precisely what the suspected criminal activity was, and regardless of whether the illegal activity occurred.

**8.3.2** A risk exists that customers could be unintentionally tipped off when a legal professional performs its CDD obligations. A customer's awareness of a possible STR or investigation could compromise future efforts to investigate the suspected money laundering or terrorist financing activity. Therefore, where a legal professional forms a suspicion that a transaction or transactions relate to money laundering or terrorist financing, a legal professional should take into account the risk of tipping off when performing the CDD process.

## 8.4 Cash reporting.

The EFIU has issued a Cash threshold reporting guideline, 2024. to A Legal Professional on this obligation and reference must be made to it. This guideline is found in the EFIU website.

## 9. SECTION 9: REGISTRATION

Over and above registration with the Prudential Supervisors all Legal Professionals are required to register their prescribed particulars with Eswatini Financial Intelligence Unit for the purposes of supervising compliance with the Money Laundering and Financing of Terrorism Prevention Act, 2011. All Legal Professionals are required to self-register on EFIU website through a link under registration.

## 10. SECTION 10: SANCTIONS FOR NON-COMPLIANCE WITH THE GUIDELINE

Non-compliance with the Guideline will expose a Legal Professional to disciplinary action in terms of section 35 of the Money Laundering and Terrorism Financing (Prevention) Act 2011. A Legal Professional should further note that compliance with the Guideline does not constitute a defence for prosecution for an offence under the MLTFP Act. Therefore, entities are encouraged to take steps to ensure that they comply with the Guideline, and the MLTFP Act.

## 11. SECTION 11: GUIDANCE AND FEEDBACK

The EFIU, in assisting a legal professional to comply with this guideline will provide feedback, which will assist a Legal Professional in applying national AML/CFT/PF measures, and in particular, in detecting and reporting suspicious transactions.

**END**

## 12. ANNEXURE 1: ML RED FLAGS

| ML Red Flags |
| --- |
| These are not exhaustive:<br>a) Customer uses an unknown intermediary to approach legal practitioner,<br>b) Customer wants to use foreign companies but does not seem to have a legitimate, legal or commercial reason for doing so,<br>c) Customer wishes to form or purchase a company with a corporate objective that is irrelevant to the customer's normal profession or activities without a reasonable explanation,<br>d) Customer performs activities that are irrelevant to his or her normal activities or profession and cannot provide a reasonable explanation,<br>e) Customer repeatedly changes legal practitioners within a short period of time without any reasonable explanation,<br>f) Customer often transfers funds or securities to a third party,<br>g) Customer is reluctant to discuss his or her financial affairs regarding behaviour that is inconsistent with his or her ordinary business practices,<br>h) Customer has a history of changing bookkeepers or accountants yearly,<br>i) Customer is uncertain about location of company records,<br>j) Customer is invoiced by organizations located in a country that does not have adequate money laundering laws and is known for high secretive banking and as a corporate tax haven,<br>k) Third party is present for all transactions but does not participate in the actual transaction,<br>l) Customer uses gatekeepers (legal practitioners) to structure deposits and purchase real estate; 13. Customer does not want to put his or her name on any document that would connect him or her with the property or uses different names on Offers to Purchase, closing documents and deposit receipts,<br>m) Customer negotiates a purchase for market value or above asking price, but records a lower value on documents, paying the difference "under the table".<br>n) Customer purchases personal use property under corporate veil when this type of transaction is inconsistent with the ordinary business practice of the customer,<br>o) Customer purchases property in the name of a nominee such as an associate or a relative (other than a spouse),<br>p) Customer purchases multiple properties in a short period and seems to have few concerns about the location, condition, and anticipated repair costs, etc. of each property,<br>q) Customer insists on providing signature on documents by fax only,<br>r) Customer frequently makes large investments in stocks, bonds, investment trusts or other securities in cash or by cheque within a short period, which is inconsistent with the normal practice of the customer,<br>s) The entry of matching buying and selling of securities or futures contracts (called match trading), creating the illusion of trading,<br>t) Customer is willing to deposit or invest at rates that are not advantageous or competitive,<br>u) Customer's documentation to ascertain identification, support income or verify employment is provided by an intermediary who has no apparent reason to be involved,<br>v) Customer seems unconcerned with terms of credit or costs associated with completion of a loan transaction; and xxiv. Customer frequently uses trust accounts for transactions where it may not make business sense to do so. |