# AML/CFT/CFP GUIDANCE NOTES FOR ATTORNEYS

**ISSUED BY THE LAW SOCIETY OF BOTSWANA IN COLLABORATION**

**WITH THE FINANCIAL INTELLIGENCE AGENCY**

<ins>**November 2021**</ins>

## Table of Contents

## Acronyms

| | |
|---|---|
| **AML/CFT/CFP** | Anti-money laundering, counter financing of terrorism/counter financing of proliferation |
| **CDD** | Customer Due Diligence |
| **CTR** | Cash transaction report |
| **DNFBP** | Designated Non-Financial Businesses and Professionals |
| **STR** | Suspicious Transaction report |
| **FATF** | Financial Action Task Force |
| **FIA** | Financial Intelligence Agency |
| **ML** | Money laundering |
| **ML/TF/PF** | Money laundering/ terrorist financing/proliferation financing |
| **PF** | Proliferation financing |
| **PIP**<br>**PEP** | Prominent Influential Person<br>Politically Exposed Person |
| **TF** | Terrorist financing |

## 1. Introduction

As financial institutions have put anti-money laundering (AML) measures into place, the risk of detection has become greater for those seeking to use the global banking system to launder criminal proceeds. Criminals now use the services provided by Designated Non-Financial Businesses and Professionals (DNFBPs) to introduce illicit funds into the financial system. DNFBPs such as Attorneys are referred to as "gatekeepers" because they wittingly or unwittingly assist criminals to launder money or finance terrorism and proliferation by providing them with advice or acting as their financial intermediaries. Three main reasons why Attorneys are exposed to misuse by criminals involved in financial offences are:

a) Engaging a lawyer adds respectability and an appearance of legitimacy to any activity being undertaken – criminals concerned about their activities appearing illegitimate will seek the involvement of a lawyer as a "stamp of approval" for certain activities.
b) The services that lawyers provide, e.g., setting up companies and trusts, or carrying out conveyancing procedures, are methods that criminals can use to facilitate money laundering.
c) Use of client trust accounts means that they are capable, even unwittingly, of "cleansing" money by simply putting it into their client account.

Attorneys have an important role in Botswana's anti-money laundering, counter financing of terrorism and counter financing of proliferation (AML/CFT/CFP) regime. In that regard, an Attorney as defined in the Legal Practitioners Act is designated as a specified party under schedule I of the Financial Intelligence Act (The Act), 2019. The Act places certain obligations on Attorneys to put measures in place to prevent their services from being used by a person to commit or to facilitate the commission of a financial offence.

However, the Act recognises that not all services provided by Attorneys are vulnerable to money laundering, terrorist financing and proliferation financing offences. Attorneys are to put AML/CFT/CFP measures in place when providing the following services:

a) Buying and selling of real estate
b) Managing client money, securities or assets
c) Management of bank savings or securities accounts
d) Organisation of contributions for the creation, operation or management of companies
e) Creation, operation or management of legal persons or for legal arrangements, trusts and the buying and selling of shares.

### 1.1. Purpose

This guidance notes is issued in in accordance with section 44 (1) (b) of the FI Act by the Law Society of Botswana in collaboration with the Financial Intelligence Agency to inform Attorneys of the risk of misuse of their business by criminals. This will assist them to play an active and informed role in the fight against Money Laundering, Terrorist Financing and Proliferation Financing as well as foster compliance with the FI Act.

## 2. Obligations of Legal Professionals

Attorneys and their firms must remain alert to money laundering, terrorism financing and proliferation financing (ML/TF/PF) risks posed by the services they provide to avoid unwittingly committing or becoming an accessory to the commission of financial offences. Attorneys and law firms must protect themselves from unwitting involvement in ML/TF/PF. Such involvement presents reputational risk to the Attorney involved, the law firm and the legal profession at large. In order to protect their businesses from misuse by criminals, Attorneys must comply with the following obligations under the Act:

### 2.1. Conduct risk assessment - *Section 11* of the Act

A risk assessment is the foundation of an effective AML/CFT/CFP programme. The management of a Law Firm must have a clear understanding of the ML/TF/PF risks associated with the services and products they offer to clients. A Law Firm shall assess the risk of commission of financial offences and take appropriate measures to manage and mitigate the identified risks. A risk assessment process has four stages[1]:

a) Identification
b) Analysis/assessment
c) Mitigation/management
d) Review and audit

When identifying aspects of the business that are vulnerable to ML/TF/PF risks; consider the following factors:

a) Customers,
b) Countries or geographic areas; and
c) Products, services, transactions or delivery channels

The risk assessment may be informed by findings of the National Risk Assessment of 2017, sectoral risk assessment reports conducted by competent authorities,[2] and any other information which may be relevant to assess the risk level particular to the Law Firm. The results of the risk assessment must inform the measures taken to protect the business from financial offences. There must be a clear link between the identified risks and the measures put in place to mitigate the risks.

### 2.2. Compliance programmes - *Section 12* of the Act

Compliance programmes are the measures and controls put in place by law firms to combat money laundering, terrorism financing and proliferation financing. The said measures and controls must be based on the conducted risk assessment such that they seek to address the identified risks. A compliance programme includes;

a) Designating a fit and proper compliance officer who should:
   i. Be at management level
   ii. Ensure implementation of the company's compliance programme.
   iii. Ensure that AML/CFT/CFP records are maintained.
   iv. Report suspicious transactions and cash transactions above the prescribed limit to the Agency.

[1] See the Financial Intelligence Agency's guidance note on risk assessment.
[2] In 2019, a multi-disciplinary Working Group conducted sector risk assessments on Legal persons, Trusts and Non-Profit Organisations. The reports are available on the Ministry of Finance and Economic Development website.

b) Vetting of relevant employees - Employee background must be checked for honesty and criminal records to ensure that the law firm has employees with the highest possible integrity.
c) Training of relevant employees - Employees must be trained on the developed AML/CFT/CFP compliance programme as well as on the ML/TF/PF red flags associated with the business of the law firm.
d) Implement an independent audit function to test the AML/CFT/CFP compliance programme.
e) Develop policies and procedures to protect the business from ML/TF for example – see Regulations 28 -31 of the Financial Intelligence Regulations:
   i. AML/CFT policies
   ii. Customer Acceptance Policy
   iii. Reporting procedures
   iv. Record keeping procedures

## 2.3. Customer Due Diligence - *section 14 -16* of the Act

Money launders, terrorists and terrorist financiers often try to hide their identity or conceal their source or intended purpose of money, but Customer Due Diligence (CDD) measures make it harder for them to do so. To minimise the ML/TF/PF risks associated with law firms, customers must be interviewed before being accepted to establish their identity and background. The law firm's compliance programme must adhere to all the CDD processes to mitigate risk.

### Why conduct CDD?

The purpose of the requirement is twofold, to:

a) Have a sufficient understanding of the customer (identification and verification).
b) Be able to properly assess the potential money-laundering, terrorist financing and proliferation financing risks associated with business relationships.

### When to conduct CDD? Section 14 of the FI Act

Attorneys are required to conduct customer due diligence measures when:

a) Establishing a business relationship or concluding a transaction with a customer/client;

b) Carrying out a transaction in excess of the prescribed amount on behalf or on the instruction of a customer/client or any person, whether conducted as a single transaction or several transactions that appear to be linked;
c) There is doubt about the veracity or adequacy of previously obtained customer/client identification data; and
d) There is suspicion of a financial offence.

## CDD must be conducted on whom? Section 16 of the FI Act

a) A customer/client
b) A beneficial owner of a customer/client
c) A person acting on behalf of a customer/client
d) A person on whose behalf a customer/client is acting[3]

Customer due diligence measures must be commensurate with the risk assessment carried out in accordance with section 11 of the Act. That is CDD requirements for a customer/client who is rated as high risk, cannot be the same as those of one rated as low risk.

## How to conduct CDD

There are different types of CDD that may be conducted. The type of CDD applied to any particular case is determined by the results of the risk assessment.

### Standard Customer Due Diligence

The information to be collected about a customer as provided for under *Regulations 5 – 9* of the Financial Intelligence Regulations of 2019. Examples of information to be collected from an individual:

a) Full name
b) Nationality
c) Identity card number and date of birth
d) Residential address
e) Contact details
f) Occupation
g) Source of funds involved in the transaction

[3] The authority to act on behalf of another person is prescribed, see Form A under the Schedule of the Financial Intelligence Act Regulations of 2019.

h) Anticipated transaction activity, including volume (amount(s)), transaction type(s), and frequency.

Enhanced Due Diligence under *section 17 of the Act*

Where the risk assessment profiles a customer as high risk or the transactions and business relationships involve countries identified as high risk by Botswana and the Financial Action Task Force (FATF) and where the customer is a Prominent Influential Person. In such cases, there is an obligation to obtain additional information from the customer.

Enhanced due diligence measures relating to Prominent Influential Person under *section 18* of the Act

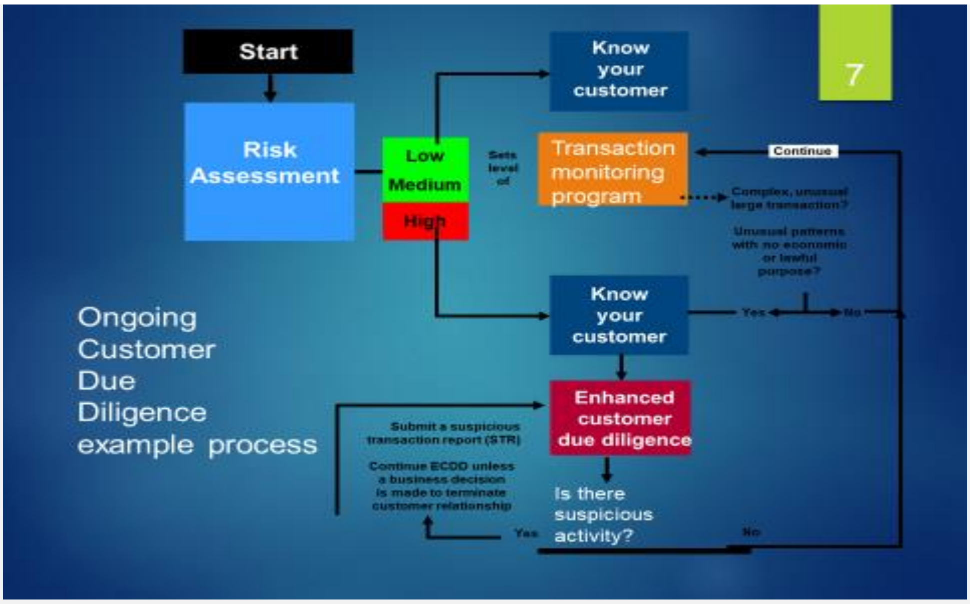
It applies to Prominent Influential Persons (PIPs), their immediate family member or close associates. PIPs have influence that puts them in positions that may be misused to launder money and finance terrorism. Therefore, Law Firms must establish whether a prospective customer is a Prominent Influential Person (PIP) or whether the beneficial owner of a prospective customer is a PIP. Where established to be PIP, the Law Firm shall:

a) Obtain senior management approval before establishing the business relationship;
b) Take reasonable measures to establish the source of wealth and source of funds of the prospective customer; and
c) Conduct enhanced ongoing monitoring of the business relationship.

Simplified due diligence under *section 24* of the Act

It is applied where the customer has been profiled as low risk by the risk assessment e.g., Government Departments, listed companies or an individual whose source of funds is traceable.

The developed risk based compliance program should state the type of CDD to be applied to certain circumstances. The Picture below is an example of application of CDD:




## Ongoing due diligence - *section 15* of the Act

Must conduct ongoing customer due diligence with respect to existing business relationships. Ongoing customer due diligence will enable the law firm to detect any changes in the customer's known profile.

## Prohibition of establishing or maintaining business relationship with terrorist or member of terrorist group - *section 23* of the Act

A specified party or accountable institution shall not establish or maintain a business relationship with a terrorist or member of a terrorist group declared under section 12 of the Counter-Terrorism Act, unless, the specified party or accountable institution has been authorised by the National Counter-Terrorism Committee.

## Customer screening - *section 25* of the Act

Law Firms are required to monitor; complex, unusual transactions; business relationships formed in a high risk jurisdiction and transactions for high risk businesses.

Screen customers against FATF high risk lists, national designations of terrorists in terms of section 12 of the Counter Terrorism Act as well as the United Nations Sanctions list. The Counter-Terrorism (Implementation of United Nations Sanctions

Resolutions) Regulations under Regulation 10, places additional obligations on specified parties, relating to implementation of UN sanctions lists.

## 3. Record keeping – section 27 and 28

### Why keep records?

Records are kept to assist with investigations. Records must be sufficient to permit the reconstruction of individual transactions so that they can be used as evidence in a prosecution. Furthermore, records should be kept to assist the law firm's ability to monitor a client's historical transaction activity and to detect unusual changes in such activity.

### Which records should be kept?

a) Records obtained through customer due diligence measures;
b) Account files; business correspondences; and
c) Results of any analysis undertaken

### How long records should be kept?

Records must be kept at least 20 years from the date a transaction is concluded and after the termination of a business relationship.

### Updating of records

Records must be kept up to date in accordance with the risk management systems of the law firm.

## 4. Reporting - Part VI

The Act places obligations on Law firms to report suspicious transactions under section 33 and large cash transactions under section 34. The reports are analysed for activities and patterns that may indicate financial and criminal offences. The analysis may lead to the prosecution of terrorists and criminals because the FIA disseminates the results of the analysis to Law Enforcement Agencies for investigation.

### 4.1. Suspicious transaction reporting – section 33

An STR must be reported to the FIA immediately and where it's not possible within 5 working days from date suspicion arose. An Attorney must report suspicion relating to the following activities:

f) Buying and selling of real estate
g) Managing client money, securities or assets
h) Management of bank savings or securities accounts
i) Organisation of contributions for the creation, operation or management of companies
j) Creation, operation or management of legal persons or for arrangements, trusts and the buying and selling of shares.

To facilitate compliance with this obligation, a law firm must:

a) Document the reporting process and procedure;
b) Establish and document suspicious transaction red flag indicators for the business;
c) Monitor and update these red flag indicators on a regular basis in order to keep up to date on the changing ML/TF/PF risks; and
d) Train employees on the STR procedure and how to identify suspicious transactions associated with the firm.

#### 4.1.1. Examples of suspicious transaction red flags or indicators[4] related to law firms:

1. The Client is:
   a. Overly secretive or evasive about: the beneficial owner and source of funds
   b. Is involved in transactions which do not correspond to his/her normal professional or business activities.
   c. Frequently changes legal structures and/or managers of legal persons
   d. Asks for short-cuts or unexplained speed in completing a transaction
2. Creation of complicated ownership structures when there is no legitimate or economic reason.

[4] Other examples are available on annexure 5 of the FATF's ***GUIDANCE FOR A RISK-BASED APPROACH FOR LEGAL PROFESSIONALS***

3. Involvement of structures with multiple countries where there is no apparent link to the client or transaction, or no other legitimate or economic reason.
4. There is an absence of documentation to support the client's story, previous transactions, or company activities.
5. Back to back property transactions, with rapidly increasing value or purchase price.
6. There are unexplained changes in instructions, especially at the last minute.
7. Requests for payments to third parties without substantiating reason or corresponding transaction.
8. The parties to the transaction are connected without an apparent business reason.
9. There are attempts to disguise the real owner or parties to the transaction.
10. The collateral being provided for the transaction is currently located in a high-risk country.
11. Private expenditure is funded by a company, business or government
12. Mortgages are repeatedly repaid significantly prior to the initially agreed maturity date, with no logical explanation.
13. The asset is purchased with cash and then rapidly used as collateral for a loan.
14. A non-profit organisation requests services for purposes or transactions not compatible with those declared or not typical for that body.

## 4.2. Cash transaction reports (CTR) – section 34

The Law Firm must report a cash transaction where the amount is equal to or above P10 000 or an equivalent amount in foreign currency. The report is made whether the cash is:

a) Paid to a customer; or
b) Received from a customer

## 4.3. How to report - Regulation 20

Reports can be sent electronically to the Agency through a system called goAML. The goAML is an internet based reporting portal used by the Financial Intelligence Agency to receive reports from specified parties. The system has two platforms; the training platform which is used by entities to practice online reporting. A law firm must register on the training platform link[5], and it is encouraged to practice reporting by using dummy data. Upon submission, the FIA checks data quality and gives the entity feedback. When the law firm is able to submit reports through the system, it must contact the FIA to register on the live platform, which is used to report actual or real cases.

### 4.4. Tipping off - section 41 (3)

A person who knows or suspects that a suspicious transaction report is being made to the Agency shall **not disclose** to any other person information or any other matter which is likely to prejudice any proposed investigation or disclose that the Agency has requested further information.

## 5. Offences

Failure to implement the AML/CFT/CFT measures means the law firm remains at risk of facilitating Money laundering/terrorist financing/proliferation financing offences. The table below shows obligations and their penalty for non-compliance:

| **Obligation/ Offence** | **Penalty (fine or term not exceeding)** |
|---|---|
| Failure to Conduct Risk assessment C/S 11(6) | P1 million |
| Failure to Implement Compliance programs C/S 12 (4) | P1 million |
| Failure to conduct customer due diligence C/S 14(4) | P1 million |
| Failure to report a STR C/S 33(6) | P5 million |
| Failure to report a CTR C/S 34(2) | P1 million |
| Tipping off C/S 41(3) & (4) | P2 million or 15 years or to both |
| Conducting business with a terrorist C/S 23(3) | P20 million<br>Suspension or revocation of licence or both |
| Failure to keep Records C/S 31(1)<br>Destroying records C/S 31(2) | P500 000 |

[5] https://www.fia.org.bw/goamltrn/Account/LogOn

## 6. Links to FATF guidance notes for Legal Professionals

1. GUIDANCE FOR A RISK-BASED APPROACH FOR LEGAL PROFESSIONALS, June 2019 - http://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Legal-Professionals.pdf
2. Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals June 2013 - http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20and%20TF%20vulnerabilities%20legal%20professionals.pdf

Approved by the Law Society of Botswana in collaboration with the Financial Intelligence Agency on the ………. day of ……………………….., 2021.

SIGNATURE :…………………………………………….
LSB **Executive Secretary**

SIGNATURE :……………………………………………..
FIA Acting **DIRECTOR GENERAL**