MINERALS COMMISSION AND FINANCIAL INTELLIGENCE CENTRE

ANTI-MONEY LAUNDERING/COUNTERING THE FINANCING OF TERRORISM & THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION (AML/CFT&P) GUIDELINES

DEALERS IN PRECIOUS METALS AND STONES IN GHANA

DECEMBER 2025

Table of Contents

FOREWORD

The extractive industry plays significant role to Ghana's economy. It contributes positively to the country's Gross Domestic Product (GDP) and the revenue generated from the total merchandise exports. The sector remains key to the country's future economic growth despite all the challenges that are faced by the industry. Presently, the sector is marred with challenges such as illegal mining, environmental degradation, inadequate local value addition to minerals produced, social conflicts from mining operations, tax evasion and potential money laundering activities.

All over the world, money laundering and terrorism financing have become threats to the economies of countries. Globally, the international organisation which is mandated to develop Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT&P) standards to effectively combat money laundering and terrorism financing is the Financial Action Task Force (FATF). The effective implementation of the FATF standards can improve the transparency of transactions and provide useful tools which are critical for combating corruption.

Generally, the mining sector has come under sustained regulatory pressure to improve its monitoring and surveillance systems with a view to preventing, detecting and responding effectively to the threat of money laundering and terrorism financing.

Therefore, taking cue from the FATF Recommendations, the Minerals Commission (MC) in collaboration with the Financial Intelligence Centre (FIC) has developed this Guidelines to assist mining lease holders and small-scale mining licence holders the Minerals and Mining Act, 2006 (Act 703) to design and implement their AML/CFT&P obligations. This Guidelines is issued in accordance with the Minerals and Mining Act, 2006 (Act 703) and Anti-Money Laundering Act, 2020 (Act 1044).

It is the hope of the Minerals Commission that this Guidelines will assist in improving transparency as well as oversight and regulatory supervision of the mining sector.

CHIEF EXECUTIVE OFFICER
MINERALS COMMISSION

CHIEF EXECUTIVE OFFICER
FINANCIAL INTELLIGENCE CENTRE

LIST OF ACRONYMS & ABBREVIATIONS

AML	-	Anti-Money Laundering
AMLRO	-	Anti-Money Laundering Reporting Officer
CDD	-	Customer Due Diligence
CFT&P	-	Countering the Financing of Terrorism and the Proliferation of Weapons of Mass Destruction
DNFBPs	-	Designated Non-Financial Businesses and Professions
DPMS	-	Dealers in Precious Metals and Stones
FATF	-	Financial Action Task Force
FIC	-	Financial Intelligence Centre
KYC	-	Know Your Client
LEA	-	Law Enforcement Agency
MC	-	Minerals Commission
ML	-	Money Laundering
PEP	-	Politically Exposed Person
STR	-	Suspicious Transaction Report
TF	-	Terrorism Financing

INTRODUCTION

Following the enactment of the Anti-Money Laundering Act, 2020 (Act 1044), the Anti-Terrorism Act, 2008 (Act 762), as amended and the Anti- Money Laundering Regulations, 2011 (L.I.1987), Ghana has intensified efforts towards the fight against money laundering and terrorism financing.

To fully realise the benefits of the Act 1044 in the mining sector, effective implementation of the collaborative measures adopted by the Minerals Commission ("MC") and the Financial Intelligence Centre ("FIC") as well as full compliance by Reporting Entities (DPMS), are essential. In accordance with section 8(1)(d) of the AML Act and Regulation 38 of the Anti-Money Laundering Regulations, 2011 (L.I.1987) ("AML Regulations"), the MC and the FIC have developed Guidelines for the Reporting Entities ("Guidelines").

This Guidelines contain relevant elements of the Act 1044 and its Regulations, Financial Action Task Force (FATF) Recommendations and other international best practices on AML/CFT&P.

PURPOSE AND OVERVIEW

Money Laundering (ML) is the process whereby criminals attempt to conceal the illegal origin and/or illegitimate ownership of property and assets that are the proceeds of their criminal activities. ML has three classical stages namely;

a) Placement - This is where ill-gotten funds are introduced into the financial and non-financial sectors.
b) Layering - This involves the concealment of sources of the ill-gotten funds through series of complex transactions.
c) Integration - This is where the laundered proceeds are placed back in the economy to create the perception of legitimacy, repatriating the laundered funds into the hands of the criminal entrepreneur, ideally with a legitimate explanation as to the source, so that they can be used without attracting suspicion.

On the other hand, Terrorism financing (TF) is defined as the process of mobilising or providing funds (legitimate or illegitimate) or resources for purposes of financing terrorist organisations or terrorist acts.

a) TF offences occurs where a person who willfully provides or collects funds by any means, directly or indirectly, with the unlawful intention that they should be used, or in the knowledge that they are to be used, in full or in part to carry out a terrorist act by a terrorist organization or by an individual terrorist.
b) Terrorism financing offences are predicate offences for ML.

Terrorism financing offences therefore apply, regardless of whether the person alleged to have committed the offence is in the same country or a different country from the one in which the terrorist or terrorist organisation is located or the terrorist act occurred or will occur.

ML and TF are global phenomena that pose major threats to international peace and security

and could seriously undermine Ghana's development and progress. For this reason, concerted global efforts are being made to combat these crimes.

Generally, Designated Non-Financial Businesses and Professions (DNFBPs), and in particular, the mining sector, have come under sustained regulatory pressure to improve their monitoring and surveillance systems with a view to preventing, detecting and responding effectively to the threats of money laundering and terrorism financing.

This Guidelines is structured into two parts; Part A is made up of the AML/CFT&P Directives and Part B provides guidance on Know Your Clients (KYC). It covers among other things the following key areas of AML/CFT&P policy:

a) designation and duties of Anti-Money Laundering Reporting Officer (AMLRO);
b) co-operation with the supervisory authority and other competent bodies;
c) customer Due Diligence (CDD);
d) monitoring and reporting of suspicious transactions;
e) reporting requirements;
f) record keeping;
g) AML/CFT&P Employee-Education Training Programme; and
h) internal controls, risk assessment, beneficial ownership, PEPs and targeted financial sanctions.

The diligent implementation of the provisions of this Guidelines will not only minimize the risk of Reporting Entities being used to launder the proceeds of crime and provide protection against reputational and financial risks which may ultimately affect the national economy. In this regard, all Reporting Entities are directed to adopt a risk- based approach in the identification and management of their ML/TF/PF risks.

OBJECTIVES

The Guidelines:

a) ensures that all Reporting Entities understand and comply with AML/CFT&P requirements and obligations.
b) mandates the MC to effectively enforce AML/CFT&P requirements and ensure compliance by all Reporting Entities.
c) provides guidance on AML/CFT&P obligations to assist Reporting Entities in the implementation of this Guidelines.

1.0 AML/CFT&P INSTITUTIONAL POLICY FRAMEWORK

Each reporting entity shall adopt policies to comply with AML/CFT&P obligations under the relevant laws and regulations.

Each Reporting Entity shall formulate and implement internal rules, procedures and other controls that will deter criminals from using its facilities for ML/TF/PF and shall ensure that its obligations under the relevant laws and regulations are always met.

1.1 RISK – BASED APPROACH IN ASSESSING ML/TF/PF RISK

Each Reporting Entity must align and integrate its AML/CFT&P risk management function with its overall risk management controls. Each Reporting Entity is required to take appropriate steps to identify, assess and understand its ML/TF/PF risks in relation to its clients in a form of a framework to guide the staff in the organisation.

In assessing ML/TF/PF risks, Reporting Entities are required to:

a) document their risk assessments and findings;
b) consider all the relevant risk factors before determining the level of overall risk, the appropriate level and type of mitigation to be applied;
c) develop and implement mitigation measures that are reflected in their internal controls;
d) keep the assessment up-to-date through a periodic review as set out in this Guidelines (including paragraph 1.5 below); and
e) provide periodic risk assessment information to the MC and FIC any time there is a review.

Additionally, Reporting Entities are required to:

a) conduct additional risk assessment as and when required by the MC within the timelines indicated by the MC.
b) be guided by the findings of the National Risk Assessment Reports which would be published by the FIC in the conduct of their respective risk assessments.
c) provide timely reporting of the ML/TF/PF risk assessment, risk profile and the effectiveness of risk control and mitigation measures to their respective Boards of Directors/Proprietors. The frequency of reporting shall be determined by their Boards/Proprietors at least once a year.

1.2 APPOINTMENT AND DUTIES OF THE ANTI – MONEY LAUNDERING REPORTING OFFICER

Each Reporting Entity shall appoint an AMLRO who shall be a key management personnel and shall operationally report to the Board/Proprietor(s) in accordance with section 50(1)(b) of the Anti-Money Laundering Act, 2020 (Act 1044), and Regulation 5(1) of L.I. 1987. The duties of the AMLRO shall include the following:

a) develop an AML/CFT&P Compliance Programme;
b) report suspicious (unusual) transactions to the FIC within 24 hours after establishing reasonable suspicion;
c) file cash transaction reports (as determined by FIC and MC under paragraph 1.21 below) with the FIC;
d) ensure that the Reporting Entity's compliance programme is implemented;
e) coordinate the training of the staff in AML/CFT&P awareness, detection methods and reporting requirements; and
f) serve both as a liaison officer with the MC and the FIC and a point-of-contact for all staff on issues relating to ML/TF&P.

See Appendix E for Submission of Statutory Returns and other reports.

For effective discharge of duties, each AMLRO:

a) shall be equipped with the relevant competence, authority and independence to implement the Reporting Entities' AML/CFT&P compliance programme.
b) should be encouraged by the Reporting Entity to acquire professional qualification in anti-money laundering and financial crime.
c) should have timely access to customer identification data, CDD information, transaction records and other relevant information for the performance of his/her obligations.

1.3 KNOW YOUR CLIENT (KYC) PROCEDURES

Each Reporting Entity shall not establish a business relationship until all relevant parties to the relationship have been identified and the nature of the business to be conducted is ascertained. Once an on-going business relationship is established, any inconsistent activity must be examined to determine whether or not there is an element or potential risk of money laundering.

1.3.1 DUTY TO OBTAIN IDENTIFICATION EVIDENCE

a) The first requirement of KYC for money laundering purposes is for the Reporting Entity to be satisfied that a prospective client is who the person claims to be.

b) Each Reporting Entity shall not carry out or agree to carry out business transactions with a client or potential client unless it is certain as to who that person actually is. If a client is acting on behalf of another (i.e. all or a part of the funds are supplied by someone else) then the Reporting Entity must verify the identity of the

client and the ultimate beneficiary.

c) Each Reporting Entity must obtain evidence of the identity of their clients or business partners.

1.3.2 NATURE AND LEVEL OF THE BUSINESS

A Reporting Entity shall obtain sufficient information on the business that its client intends to undertake, including the expected or predictable pattern of transactions.

a) The information collected at the outset for this purpose should include:
   i. origin of the funds to be used during the business transaction/relationship; and
   ii. details of client's occupation/employment/business activities such as company profile, details of key management personnel and/or directors and/or shareholders.

b) Each Reporting Entity shall take reasonable steps to keep the information up to date. Information obtained during any meeting, discussion or other communication with the client shall be recorded and kept in the client's file to ensure, as far as practicable, that current client information is readily accessible to the AMLRO or relevant regulatory bodies.

1.3.3 RISK-BASED APPROACH TO THE KYC REQUIREMENTS

Each Reporting Entity shall take a risk-based approach to the KYC requirements. It shall also document the number of times to verify the clients' records during the relationship, the identification evidence required and when additional checks are necessary. In respect of a private company or a partnership, focus shall be on the:

a) principal owners/controllers and their identities shall also be verified.

b) identification evidence collected at the outset should be viewed against the inherent risks in the business or service.

1.3.4 ESTABLISHMENT OF IDENTITY

a) The client identification process shall not end at the point of establishing the relationship but shall continue for as long as the business relationship subsists. The process of confirming and updating identity, and the extent of obtaining additional KYC information collected will however differ from one Reporting Entity to another.

b) The general principles for establishing the identity of both legal and natural persons and the procedures on obtaining satisfactory identification evidence set out in this Guidelines is not exhaustive.

1.3.5 WHAT IS IDENTITY?

a) Identity generally means a set of attributes such as name(s) used, date of birth,

and the residential address, including the digital address at which the client can be located. These are features that can uniquely identify a natural or legal person.

b) In the case of a natural person, the date of birth of that client shall be obtained as an important identifier in support of their name.

c) Where an international passport, national identity card, or any other acceptable identification as provided in this Guidelines is taken as evidence of identity, the number, date, and place/country of issue as well as expiry date shall be recorded.

1.3.6 WHEN MUST IDENTITY BE VERIFIED?

a) Identity shall be verified whenever a business relationship is to be established, during one-off transaction, or when a series of linked transactions take place.

b) Once identification procedures have been satisfactorily completed and the business relationship established, as long as contact or activity is maintained and records concerning that client are complete and kept up-to-date, no further evidence of identity is needed when another transaction or activity is subsequently undertaken unless there is a change in the persons whose identity were previous verified (e.g. new people become involved in the business relationship, or if any of the previously verified individuals are replaced or submitted).

1.3.7 WHOSE IDENTITY MUST BE VERIFIED?

a) Clients - sufficient evidence of the identity shall be obtained to ascertain that the client is the very person they claim to be.

b) The person acting on behalf of another - the obligation is to obtain sufficient evidence of identities of the two persons involved.

1.3.8 TIMING OF IDENTIFICATION REQUIREMENTS

a) An acceptable time-span for obtaining satisfactory evidence of identity will be determined by the geographical location of the parties and whether it is possible to obtain the evidence before commitments are entered into or money changes hands. However, any occasion when business is conducted before satisfactory evidence of identity has been obtained must be exceptional and can only be those circumstances justified with regard to the risk.

b) The failure or refusal by a client to provide satisfactory identification evidence within a reasonable time-frame without adequate explanation may lead to a suspicion that the client is engaged in money laundering. Where a client is suspected of engaging in ML, the Reporting Entity shall therefore make a STR to the FIC based on the information in its possession.

c) Each Reporting Entity shall have in place written and consistent policies for

unwinding a transaction where satisfactory evidence of identity cannot be obtained.

d) Each Reporting Entity shall respond promptly to inquiries made by competent authorities.

1.3.9 CERTIFICATION OF IDENTIFICATION DOCUMENTS

a) In order to guard against the dangers of postal interception and fraud, prospective clients should not be asked to send by post, originals of their personal identity documents such as international passport, identity card, driving licence etc.

b) Where there is no face-to-face contact with the client and documentary evidence is required, certified copies of the documentary evidence should be provided by the client to the Reporting Entities. A document can be certified by a notary public. The notary public certifying the documentary evidence must:

   i. be known and capable of being contacted, if necessary;

   ii. not be related to the client; and

   iii. not be living at the same address.

c) In the case of foreign nationals, the copy of international passport, national identity card or documentary evidence of his/her address shall be certified by:

   i. the embassy/high commission or consulate of the country of issue; or
   ii. a notary public.

d) Certified copies of identification evidence are to be stamped, dated, signed and sealed "Certified to be a true copy of the original seen by me" by a notary public. The full name, occupation, professional address and telephone number of the person certifying the document must be printed under their signature.

e) Each Reporting Entity shall demand the presentation of a national identity card from the individual concerned before providing the relevant service to the individual in accordance with Regulation 7 of the National Identy Register Regulations, 2012, L.I. 2111

1.3.10 RECORDING IDENTIFICATION EVIDENCE

a) Records of the supporting evidence and methods used to verify identity are required to be retained for a minimum period of five (5) years after the end of the business transaction/relationship.

b) Where the supporting evidence could not be copied at the time it was presented, the reference numbers and other relevant details of the identification evidence shall be recorded to enable the documents to be obtained later. Confirmation shall be provided that the original documents were seen by certifying either on the

photocopies or on the record that the details were taken down as evidence.

c) Where checks are made electronically, a record of the actual information obtained or of where it can be re-obtained must be retained as part of the identification evidence. Such records will make the reproduction of the actual information that would have been obtained before, less cumbersome.

d) A Reporting Entity may appoint a third party to keep records on its behalf and such appointment must with the data protection laws of Ghana and where applicable the data protection laws of the jurisdiction in which the third party operates.

e) Despite subsection (d), ultimate responsibility to comply with the requirements of this section shall not be delegated and remains at all times with the Reporting Entity that relied on the appointed person.

f) Each Reporting Entity shall not outsource record keeping to a third party in another jurisdiction where that jurisdiction is listed in domestic and international sanctions lists.

g) A Reporting Entity that appoints a person to keep records on its behalf shall within seven days, inform the FIC and MC of the appointment in writing.

1.3.11 ACQUISITION OF ONE REPORTING ENTITY BY ANOTHER

a) When one Reporting Entity acquires the business of another Reporting Entity, it is not necessary for the identity of all the existing clients to be re-verified, provided that all the underlying clients' records are acquired with the business. It is, however, important to carry out due diligence enquiries to confirm that the acquired institution had conformed to the requirements in this Guidelines.

b) Verification of identity should be undertaken as soon as it is practicable for all the transferred clients who were not verified by the transferor in line with the requirements for existing clients, where:

   i. the Anti-Money Laundering procedures previously undertaken have not been in accordance with the requirements of this Guidelines;

   ii. the procedures cannot be checked; or

   iii. where the client records are not available to the acquiring Reporting Entity.

1.3.12 SANCTIONS FOR NON-COMPLIANCE WITH KYC

Failure to comply with the provisions contained in this Guidelines will attract appropriate sanctions in accordance with existing laws. In line with this, MC shall make distinction between a breach, deficiency and recommendation.

a) Breaches of the Act 1044 - The Reporting Entity has failed to meet the requirements of the Act 1044. The MC considers the breach to be a material issue

and/or a systemic issue that requires immediate steps to be taken to remedy the breach. This will attract immediate penalties or sanctions from MC as set out in the AML/CFT&P Administrative Penalties and Sanctions Regime.

b) Deficiency - The Reporting Entity has failed to meet the standard requirements of the Act 1044. MC considers supervisory action is required to achieve ongoing compliance within a specified timeline stated by MC. Failure to comply within the specified timeline shall attract administrative penalties or sanctions from MC as set out in the AML/CFT&P Administrative Penalties and Sanctions Regime.

c) Recommendations - MC considers it best practice for Reporting Entity to consider and implement the appropriate changes in line with MC recommendations. These recommendations do not constitute regulatory action.

1.4 CUSTOMER DUE DILIGENCE (CDD)

CDD is the identification and verification of both a client and beneficiary including continuous monitoring of their business relationship with the Reporting Entity. Reporting Entities are not permitted to conduct business with anonymous clients or clients with fictitious names.

1.4.1 APPLICATION OF CDD MEASURES

Each Reporting Entity shall undertake CDD measures when:

a) business relationships are established;

b) carrying out occasional transactions. This may include transactions carried out in a single operation or several operations that appear to be linked;

c) there is a suspicion of ML/TF/PF, regardless of any exemptions or any other thresholds referred to in this Guidelines; or

d) there are doubts about the veracity or adequacy of previously obtained client's identification data.

A Reporting Entity shall not commence business relationship or perform a transaction with a client where the requirement under (a), (b), (c) or (d) above have not been met.

A Reporting Entity shall submit a Suspicious Transaction Report (STR) to the FIC within twenty-four hours where a prospective client fails to submit information required under the CDD measures.

A Reporting Entity that has already commenced a business relationship shall terminate the business relationship where a client fails to submit additional information required under the CDD measures and submit an STR to the FIC within twenty-four hours.

1.4.2 CDD PROCEDURES

a) Each Reporting Entity shall identify its clients (whether permanent or occasional; natural

or legal persons; or legal arrangements) and verify the clients' identities using reliable, independently sourced documents, data or information. Each Reporting Entity is required to carry out the full range of the CDD procedures in this Guidelines. However, in reasonable circumstances, a reporting entity can apply the CDD procedures on a risk- based approach.

b) The nature of clients' information to be obtained and the identification data to be used to verify the information are provided in Appendix B.

In respect of clients that are legal persons or legal arrangements, each Reporting Entity shall:

i. verify the identity of the person purporting to have been authorized to act on behalf of such a client and

ii. verify the legal status of the legal person or legal arrangement by obtaining proof of incorporation from the Office of the Registrar of Companies (ORC) or similar evidence of establishment or existence and any other relevant information.

c) Each Reporting Entity shall identify a beneficial owner and take reasonable measures to verify their identity using relevant information or data obtained from a reliable source to satisfy itself that it knows who the beneficial owner is.

d) Each Reporting Entity shall in respect of all clients determine whether or not a client is acting on behalf of another person. Where the client or any other third party is acting on behalf of another person, the Reporting Entity shall take reasonable steps to obtain sufficient identification data and to verify the identity of that other person as pertains in (a) above.

e) Each Reporting Entity shall take reasonable measures in respect of clients that are legal persons or legal arrangements to:

ii. understand the ownership and control structure of such a client; and

ii. determine the natural persons that ultimately own or control the client.

The natural persons include those persons who exercise ultimate and effective control over the legal person or arrangement.

For companies - The natural persons are those who own the controlling interests and those who comprise the mind and management of the company; and

For trusts – The natural persons are the settlor, the trustee and person exercising effective control over the trust and the beneficiaries.

Where the client or the owner of the controlling interest is a public company subject to regulatory disclosure requirements (i.e. a public company listed on a recognised stock exchange) it is not necessary to identify and verify the identity of the shareholders of such a public company.

f) The ongoing due diligence would include scrutinising the transactions undertaken by

clients throughout the course of their relationship with the Reporting Entity to ensure that the transactions being conducted are consistent with the Reporting Entity's knowledge of the client, its business and risk profiles and the source of funds (where necessary). In keeping with this requirement, reporting entities shall have a monitoring mechanism to identify all transactions with the view to detecting suspicious transactions by their clients.

g) Each Reporting Entity shall ensure that documents, data or information collected under the CDD process are kept up-to-date and relevant by undertaking reviews of existing records, particularly, the records in respect of higher-risk business relationships or client categories.
h) Each Reporting Entity shall screen all clients (existing and new) against all domestic sanction list, UN sanction list (https://www.un.org/securitycouncil/content/un-sc-consolidated-list) and third-party sanction list. Entities and individuals on these lists should be documented and reported to the FIC immediately. Where a Reporting Entity realizes that it has wrongly submitted details of persons cited on the UN List, the Reporting Entity shall immediately inform the FIC for the necessary remediation measures to be taken.

1.5 ML/TF/PF RISK ASSESSMENT AND PROFILING

Reporting Entities shall prepare an internal risk assessment framework to identify, assess and take effective action to mitigate their ML/TF/PF risks.

The concept of Reporting Entity assessment and management of their ML/TF/PF risks, including assignment of risk rating scores of business/client ML/TF/PF risks into the categories of "low risk", "medium risk" and "high risk" is outlined in this section and expanded in Appendix D. The notes relating to risk assessment, client risk factors, geographic or country risk factors, product, service and delivery channel risk factors and risk variables are primarily sourced from the FATF Recommendation 1 on Risk Assessment and Recommendation 10 on Customer Due Diligence and the accompanying Interpretative Notes.

The same risk management principles that the Reporting Entity uses in traditional operational areas should be applied to assessing and managing AML/CFT&P risk. A well-developed risk assessment and rating will assist in identifying the Reporting Entity's AML/CFT&P risk profile and properly rating its business/client ML/TF/PF risk. Understanding the risk profile enables the reporting entity to apply appropriate risk management processes to the AML/CFT&P compliance programme to mitigate risk. This risk assessment process enables Management to better identify and mitigate gaps in the Reporting Entity's controls.

AML/CFT&P risk assessment and rating generally involves two steps:

i. identify the specific risk categories (i.e., for clients, countries or geographic areas; type of mineral, volume of transactions or delivery channels) unique to the

Reporting Entity; and

ii. conduct a more detailed analysis of the data identified to better assess the risk within these categories and risk rating each client.

1.6 HIGHER-RISK CATEGORIES OF CLIENTS

Each Reporting Entity shall perform enhanced due diligence for higher-risk categories of clients, business relationships or transactions.

Examples of higher-risk client categories include:

a) non-resident clients;
b) politically exposed persons (PEPs);
c) cross-border business relationships; and
d) any client deemed high risk by the Reporting Entity.

A more extensive list of higher-risk situations can be found at Annex E.

1.7 LOWER-RISK CATEGORIES OF CLIENTS

Low risks occur in circumstances where:

a) the risk of ML/TF/PF is lower
b) information on the identity of the client and the beneficial owner of a client is publicly available
c) adequate checks and controls exist elsewhere in other public institutions.

In circumstances of low-risks, Reporting Entities shall apply the Simplified or Reduced CDD procedures to identify and verify the identity of their clients and the beneficial owners. These procedures include:

a) put in place the basic customer due diligence measures such as obtaining identification records.
b) reducing the frequency of customer identification updates.
c) reducing the degree of ongoing monitoring of due diligence measures.

Simplified CDD procedures should not apply to a client whenever there is suspicion of money laundering or terrorism financing and proliferation or specific higher-risk scenarios. In such a circumstance, enhanced due diligence is mandatory.

1.8 TIMING OF VERIFICATION

(a) Each Reporting Entity shall verify the identity of regular and occasional clients and beneficial owners before or during the course of establishing a business relationship or conducting transactions with them.

(b) Reporting Entities are permitted to complete the verification of the identity of a client and

beneficial owner following the establishment of the business relationship, only when:

i. this can take place as soon as reasonably practicable;
ii. it is essential not to interrupt the normal business conduct of the client; and
iii. the ML risks can be effectively managed.

(c) Where a client is permitted to establish a business relationship prior to verification, Reporting Entities are required to adopt risk management procedures concerning the conditions under which this may occur. These procedures include a set of measures such as:

i. limiting the number, types and/or amount of transactions that can be performed;
ii. monitoring large or complex transactions being carried out outside the expected norms for that type of relationship.

1.9 EXISTING CLIENTS

a) Each Reporting Entity shall apply CDD requirements to existing clients on the basis of materiality and risk and to continue to conduct due diligence on such existing relationships at appropriate times.

b) Each Reporting Entity shall update CDD requirements:

i. every year for higher-risk clients
ii. every two years for moderate-risk clients
iii. every three years for low-risk clients

c) Circumstances under which immediate update of CDD is required by a Reporting Entity is when:

i. a transaction of significant value takes place,
ii. client documentation requirements change substantially,
iii. there is a material change in the way that business is conducted
iv. the Reporting Entity becomes aware that it lacks sufficient information about an existing client, and
v. the client's existing identification documents have expired.

1.10 POLITICALLY EXPOSED PERSONS (PEPs)

a) PEPs are persons who are or have been entrusted with prominent public functions both in Ghana or in foreign countries and people or entities associated with them. PEPs also include persons who are or have been entrusted with prominent functions by international organisations. Examples of PEPs include;

i. heads of state or government;
ii. ministers of State;
iii. politicians;
iv. senior political party officials;

v. senior public officials;
vi. senior judicial officials;
vii. senior military officials;
viii. chief executives of state-owned companies/corporations;
ix. immediate family members or close associates of PEPs.

b) Each Reporting Entity shall, in addition to performing CDD procedures, put in place appropriate risk management systems to determine whether a potential client or existing client or the beneficial-owner is a PEP. These may include the use of a commercial database, internet searches and PEP's declaration form.

c) Each Reporting Entity shall maintain a PEP register and submit a PEP List quarterly to the FIC.

d) An officer acting on behalf of a Reporting Entity shall obtain Senior Management's approval before establishing a business relationship with PEP. The business owner can be considered senior management.

e) Where a client has been accepted or has an ongoing relationship with a Reporting Entity and the client or beneficial-owner is subsequently found to be or becomes a PEP, an officer acting on behalf of the Reporting Entity shall obtain Senior Management's approval in order to continue the business relationship.

f) Each Reporting Entity shall take reasonable measures to establish the source of wealth and the sources of funds of clients and beneficial-owners identified as PEPs and report all anomalies immediately to the FIC and other relevant authorities.

g) A Reporting Entity in business relationships with PEPs is required to conduct enhanced ongoing monitoring of that relationship. In the event of identifying any transaction that is abnormal, the Reporting Entity is required to report immediately to the FIC and other relevant authorities.

1.11 CROSS-BORDER BUSINESS ACTIVITIES

In relation to cross-border business activities, each Reporting Entity shall, in addition to performing the normal CDD procedures, take the following measures:

a) gather sufficient information about the overseas business partner to understand fully the nature of its business and to determine from publicly available information the reputation of the partner, including whether or not it has been a subject to an ML/TF/PF investigation or regulatory action or criminal prosecution.

b) obtain approval from Senior Management before establishing business transactions.

1.12 NEW TECHNOLOGIES AND NON-FACE-TO-FACE TRANSACTIONS

a) Each Reporting Entity shall have policies in place or take such measures as may be necessary to prevent the misuse of technological developments in ML/TF/PF schemes.

b) Each Reporting Entity shall have policies and procedures in place to address any specific risks associated with non-face-to-face business relationships or transactions. These policies

and procedures shall be applied automatically when establishing client relationships and conducting ongoing due diligence. Measures for managing the risks should include specific and effective CDD procedures that apply to non-face-to-face clients such as setting value and transaction limits, verification of identification documents.

1.13 MAINTENANCE OF RECORDS ON TRANSACTIONS

a) Each Reporting Entity shall maintain records of the identification data, client files and business correspondence in accordance with Section 32 of Act 1044.

b) Examples of the necessary components of transaction records include client's and beneficiary's names, addresses, nature and date of the transaction, currency and amount involved and the identification document of the client provided for the transaction.

c) Each Reporting Entity shall ensure that all client transaction records and information are available on a timely basis to the MC and FIC.

d) The above requirements apply whether the business relationship is ongoing or has been terminated.

1.14 MONITORING AND REPORTING OF SUSPICIOUS TRANSACTIONS AND TERRORISM FINANCING

For the purpose of this Guidelines, a suspicious transaction may be defined as one that is unusual because of its size, volume, type or pattern or otherwise suggestive of known money laundering, terrorism financing or proliferation financing methods. It includes such a transaction that is inconsistent with a client's known legitimate business or personal activities or that lacks an obvious economic rationale.

Each Reporting Entity shall pay special attention to all complex, unusual large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose.

Each Reporting Entity is required to examine as far as possible the background and purpose of such transactions and report any suspicion to the FIC within 24 hours.

1.15.1 SCOPE OF UNLAWFUL ACTIVITIES/PREDICATE OFFENCES

Each Reporting Entity shall identify and report to the MC and the FIC, the proceeds from unlawful activities undertaken by clients of the Reporting Entity. For the avoidance of

doubt, the unlawful activities include the following:

i. participation in an organised criminal group and racketeering;
ii. terrorism, including terrorism financing;
iii. trafficking in human beings and migrant smuggling;
iv. sexual exploitation, including sexual exploitation of children;
v. illicit trafficking in narcotic drugs and psychotropic substances;
vi. illicit arms trafficking;
vii. illicit trafficking in stolen and other goods;
viii. corruption and bribery;
ix. fraud;
x. counterfeiting currency;
xi. counterfeiting and piracy of products;
xii. environmental crime;
xiii. murder, grievous bodily injury;
xiv. kidnapping, illegal restraint and hostage-taking;
xv. robbery or theft;
xvi. smuggling;
xvii. tax Evasion;
xviii. extortion;
xix. forgery;
xx. piracy;
xxi. insider trading and market manipulation;
xxii. cyber crime.

1.15.2 INSTITUTIONAL POLICY

a) Each Reporting Entity shall have a written policy framework that would guide and enable its staff to monitor, recognise and respond appropriately to suspicious transactions. A list of Money Laundering Indicators and "Red Flags" is provided in Appendix C to this Guidelines.

b) Each Reporting Entity shall designate an officer appropriately as the AMLRO to; inter alia supervise the monitoring and reporting of suspicious transactions.

c) Each Reporting Entity should be alert to the various patterns of conduct that have been known to be suggestive of money laundering and maintain a checklist of such transactions which should be disseminated to the relevant staff.

d) When any staff of a Reporting Entity detects any "red flag" or suspicious money laundering activity, the staff is required to promptly report to the AMLRO. The entity and its staff shall maintain confidentiality in respect of such investigation and any suspicious transaction report that may be filed with the competent authority. This action is, however, in compliance with the provisions of the Act 1044 which criminalises "tipping

off".

e) A Reporting Entity that suspects or has reason to suspect that funds are the proceeds of unlawful activity or are related to terrorism financing shall report within 24 hours, its suspicions to the FIC. All suspicious transactions, including attempted transactions are to be reported regardless of the amount involved and this should apply regardless of whether they are thought, among other things, to involve tax matters. The reporting should be filed with FIC through a prescribed medium.

f) Each Reporting Entity, its directors, owners, and employees (permanent and temporary) is prohibited from disclosing the fact that a report is required to be filed or has been filed with the competent authorities to anyone, particularly the individual who is subject to the suspicious transaction report.

1.16 INTERNAL CONTROLS, COMPLIANCE AND AUDIT

a) Each Reporting Entity shall establish and maintain written internal procedures, policies, and controls to prevent ML/TF/PF and to communicate these to its employees. These procedures, policies, and controls should cover all AML/CFT&P obligations, including CDD, record keeping, the detection and reporting of unusual and suspicious transactions, targeted financial sanctions, politically exposed persons, risk assessment, among other things.

b) Each Reporting Entity is therefore required to develop programmes against ML/TF/PF to include:

   i. the development of internal policies, procedures, and controls, including appropriate compliance management arrangements and adequate screening procedures to ensure high standards when hiring employees;

   ii. ongoing employee-education training programmes to ensure that employees are kept informed of new developments, including:

      a. information on current ML and TF techniques, methods, and trends;
      b. clear explanation of all aspects of AML/CFT&P laws and obligations; and
      c. requirements concerning CDD and suspicious transaction reporting.

   iii. the employee-education training shall be held at least once a year and shall be documented.

c) Each Reporting Entity shall have an independent audit function to test compliance with the procedures, policies, and controls annually.

1.17 AML/CFT&P EMPLOYEE-EDUCATION TRAINING PROGRAMME

1.17.1 INSTITUTIONAL POLICY

a) Each Reporting Entity is required to submit annual AML/CFT&P employee-

education training programme for the ensuing year to the MC and FIC not later than the 31st of December every year.

b) Each Reporting Entity shall design employee-education training programmes not only to make employees fully aware of their obligations but also to equip them with relevant skills required for the effective discharge of its AML/CFT&P tasks.

c) The timing, coverage and content of the employee-education training programme should be tailored to meet the perceived needs of each Reporting Entity. A comprehensive training programme is required to encompass all staff.

d) The employee-education training programme is required to be developed under the guidance of the AMLRO in collaboration with the Executive Management. The basic elements of the employee training programme are expected to include:

i. AML Regulations and offences
ii. the nature of money laundering
iii. ML "red flags" and suspicious transactions, including trade based money laundering typologies
iv. reporting requirements
v. customer due diligence
vi. risk-based approach to AML/CFT&P regime
vii. record keeping and retention policy.

e) Each Reporting Entity shall fully participate in all AML/CFT&P interactive programmes organised by MC or FIC.

f) Each Reporting Entity shall submit annual report on their level of compliance to the MC and FIC.

1.18 PROTECTION OF STAFF WHO REPORT VIOLATIONS

a) Each Reporting Entity shall direct its employees in writing and ensure that they always co-operate fully with the MC, FIC and LEAs. They are also required to make it possible for directors, owners and employees to report any violations of the Reporting Entity's AML/CFT&P compliance programme to the AMLRO. Where the violations involve the AMLRO, employees are required to report such to a designated higher authority.

b) Each Reporting Entity shall inform its employees in writing to make such reports confidential and that they will be protected from victimisation.

1.19 APPROVAL OF THE AML/CFT&P COMPLIANCE MANUAL

The ultimate responsibility for AML/CFT&P compliance is placed on the Board or the highest decision-making body of the Reporting Entity in Ghana. It is therefore, required that the Board or the highest decision-making body ensures that a

comprehensive operational AML/CFT&P compliance manual is formulated and approved. Copies of the approved manual above are to be forwarded to the FIC and MC within two (2) weeks of the release of the manual. Annual reports on the AML/CFT&P compliance status of the institution shall be presented to the Board or the highest decision-making body for its information and necessary action.

1.20 CULTURE OF COMPLIANCE

Each Reporting Entity shall have a comprehensive AML/CFT&P compliance programme based on the results of its risk assessment to guide its compliance efforts and to ensure the diligent implementation of its AML/CFT&P policy.

1.21 OTHER FORMS OF REPORTING

Each Reporting Entity shall report to the FIC all cash transactions within Ghana in any currency and with a threshold of the Ghana Cedi equivalent of Fifteen Thousand United States Dollars and above.

1.22 HIGHER RISK COUNTRIES

a) Each Reporting Entity shall give special attention to business relationships and transactions with persons (including legal persons) from or in countries which do not or insufficiently apply the AML/CFT&P measures and have been identified on the FATF grey and black lists or other similar lists.

b) Reporting Entities that conduct business with high-risk countries shall perform enhanced CDD measures as follows:

i. obtaining additional information of the client (eg. occupation, volume of assets) and updating more regularly the identification data of client and beneficial owner.

ii. obtaining additional information on the intended nature of the business relationship

iii. obtaining information on the source of funds or source of wealth of the client

iv. obtaining information on the reasons for intended or performed transactions

v. obtaining the approval of senior management to commence or continue the business relationship

vi. 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.

c) Reporting Entities that conduct business with high-risk countries shall immediately report the business transactions to FIC and MC.

1.23 OVERSEAS ENTITIES

a) Each Reporting Entity shall ensure that their foreign branches and subsidiaries or parent companies observe group AML/CFT&P procedures consistent with the provisions of the Guidelines and to apply them to the extent that the local/host country's laws and regulations permit.

b) Each Reporting Entity shall ensure that the above principle is observed with respect to their branches and subsidiaries in countries which do not or insufficiently apply such requirements as contained in the Guidelines. Where these minimum AML/CFT&P requirements and those of the host country differ, the overseas entities in the host country are required to apply the higher standards and such must be applied to the extent that the host country's laws, regulations or other measures permit.

c) Each Reporting Entity shall implement group-wide programmes against ML/TF/PF, which should be applicable, and appropriate to, all branches and majority-owned subsidiaries of the Reporting Entity. These measures include:
   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-education training programme;
   iv. an independent audit function to test the system;
   v. policies and procedures for sharing information required for the purposes of CDD and ML/TF/PF risk management;
   vi. the provision, at group-level compliance, audit and/or AML/CFT&P functions, of clients and transaction information from branches and subsidiaries when necessary for AML/CFT&P purposes; and
   vii. adequate safeguards on the confidentiality and use of information exchanged.

d) Each Reporting Entity shall inform the MC in writing when its overseas entity is unable to observe the appropriate AML/CFT&P procedures because it is prohibited by the host country's laws, regulations or other measures.

e) Each Reporting Entity is subject to these AML/CFT&P principles, and shall therefore apply consistently the CDD procedures at its group level, taking into account the activity of the clients with the various branches and subsidiaries.

1.24 COOPERATION WITH COMPETENT AUTHORITIES

Each Reporting Entity shall comply promptly with all requests for information on money laundering and terrorism financing made pursuant to the law and regulations and provide such information to the MC, FIC and other relevant competent authorities.

Each Reporting Entity's procedures for responding to authorised requests for information on money laundering and terrorism financing shall be as follows:

a) search immediately the reporting entity's records to determine whether it maintains or has maintained any business relationship, engaged in any transaction with each individual, entity, or organisation named in the request;
b) report promptly to the requesting authority, the outcome of the search; and
c) protect the security and confidentiality of such requests.

1.25 ACCESS TO INFORMATION

Notwithstanding a Reporting Entity's internal policies relating to clients' confidentiality, competent authorities in accordance with the provisions in Act 1044 shall have access to information in order to perform their functions in combating ML/TF/PF. In so doing, a competent authority may share the information with other competent authorities (either domestically or internationally).

1.26 SANCTIONS

In addition to the administrative and regulatory sanctions that may be imposed by MC as indicated in Act 703 and its Regulations and the AML/CFT&P Administrative Penalties and Sanctions Regime, particulars of the breaches of the Guidelines by Reporting Entities or individual(s) shall be referred to the appropriate law enforcement agency for further action.

APPENDIX A

DEFINITION OF TERMS

For the proper understanding of the Guideline, certain terms used within are defined as follows:

Terms	Definition
Beneficial owner	This refers to the natural person(s) who ultimately owns or controls a client and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.
Business Entity	This includes (a) An individual licensed to carry out a business, (b) a limited liability company, or (c) a partnership
Business Relationship	This is any arrangement between the Reporting Entity and the applicant for business whose purpose is to facilitate the carrying out of transactions between the parties on a "frequent or regular" basis.
Client	The person or company seeking to establish a business relationship or an occasional customer undertaking a "one-off" transaction whose identity must be verified.
Cross-border business activities	This means any transaction where the reporting entity and overseas business partners are located in different jurisdictions. This term also refers to any chain of business activities that has at least one cross-border element.
Dealers in Precious Metals and Stones (DPMS)	Individuals or entities involved in the trading of precious metals and precious stones. This includes a wide range of participants, from those who produce these materials at mining operations to intermediaries, buyers, and sellers in the secondary market.

Financial Action Task Force (FATF).	The Global Standard setting body for Anti-money Laundering and Countering of Terrorism Financing
The FATF Recommendations	This refers to the Forty Recommendations of the Financial Action Task Force (FATF).

Legal arrangements	This refers to express trusts or other similar legal arrangements.
Legal persons	This refers to bodies corporate, foundations, partnerships, or associations, or any similar bodies that can establish a permanent client relationship with a Reporting Entity or otherwise own property.
One-off Transaction	This means any transaction carried out other than in the course of an established business relationship. It is important to determine whether a client is undertaking a one-off transaction or whether the transaction is or will be a part of a business relationship as this can affect the identification requirements.
Proceeds	It refers to any property derived from or obtained, directly or indirectly, through the commission of an offence.
Property	It means assets of every kind, whether corporeal or incorporeal, moveable or immoveable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in such assets.
Reporting Entities	This refers to: (a) Mining Lease holders; (b) Small scale mining licence holders
Risk	This refers to the threats and vulnerabilities of money laundering and/or terrorism financing.

Settlor	These are persons or companies who transfer ownership of their assets to trustees by means of a trust deed. Where the trustees have some discretion as to the investment and distribution of the trust's assets, the deed may be accompanied by a non-legally binding letter setting out what the settlor wishes to be done with the assets.

Terrorist	It refers to any natural person who: a. Commits or attempts to commit terrorist acts by any means, directly or indirectly, unlawfully and willfully; b. Participates as an accomplice in terrorist acts; c. Organises or directs others to commit terrorist acts; or d. Contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.

Terrorist act	A terrorist act includes: An act which constitutes an offence within the scope of, and as defined in one of the following treaties: Convention for the Suppression of Unlawful Seizure of Aircraft (1970), Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971), Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents (1973), International Convention against the Taking of Hostages (1979), Convention on the Physical Protection of Nuclear Material (1980), Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1988), Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (1988), Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf (1988), and the International Convention for the Suppression of Terrorist Bombings (1997); and any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act.
Terrorism financing	This includes the financing of terrorist acts and of terrorists and terrorist organisations.
Terrorism financing offence	This includes the wilful provision or collection of funds/resources by any means, directly or indirectly, with the unlawful intention that this should be used, or in the knowledge that they are to be used in full or in part: a. To carry out a terrorist act; b. By a terrorist organization; c. By an individual terrorist.

Terrorist organisation	Refers to any group of terrorists that: a. Commits or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and willfully; b. Participates as an accomplice in terrorist acts; c. Organises or directs others to commit terrorist acts; or d. Contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.
Third Party Sanction List	This includes: a. OFAC List b. Interpol c. EU Sanctions List
Trustee	Trustees, include paid professionals or companies or unpaid persons who hold the assets in a trust fund separate from their own assets. They invest and dispose of them in accordance with the settlor's trust deed, taking account of any letter of wishes.

APPENDIX B

INFORMATION TO ESTABLISH IDENTITY OF NATURAL PERSONS

For natural persons the following information should be obtained, where applicable:

i. legal name and any other names used by the prospective client;
ii. location, including important landmarks close to the prospective client's residence;
iii. digital address;
iv. telephone and mailing address;
v. date and place of birth;
vi. nationality;
vii. hometown;
viii. occupation, position held and employer's name;
ix. identity document; and
x. signature.

The Reporting Entity should verify this information by at least one of the following methods:

- confirming the date of birth from an official document (e.g. birth certificate, passport, social security records, national identity card,);
- confirming the permanent address (e.g. utility bill, tax assessment, bank statement, a letter from a public authority);
- contacting the client by telephone, by letter or by e-mail to confirm the information supplied after the business relationship has been established (e.g. a disconnected phone, returned mail, or incorrect e-mail address should warrant further investigation);
- confirming the validity of the official documentation provided through certification by an authorised person (e.g. embassy official, notary public) and
- any other means of verification that is deemed appropriate.

Reporting Entities should apply the same standard of identification and verification in respect of non-face-to-face clients.

APPENDIX C

MONEY LAUNDERING AND TERRORISM FINANCING -"RED FLAGS"

Monitoring and reporting of suspicious transactions is key to AML/CFT&P effectiveness and compliance. Reporting Entities are therefore required to put in place effective and efficient transaction monitoring programmes to facilitate the process. Although the types of transactions which could be used for money laundering are numerous, it is possible to identify certain basic features which tend to give reasonable cause for suspicion of money laundering.

Red flags and indicators are specific activities behind certain activities, transactions, actions and events that may lead to suspicion and may require further examination and monitoring.

The indicators and red flags differ depending on the extent of the money laundering or suspected terrorist financing activities. While the indicators represent events that may or may not indicate the existence of money laundering or terrorist financing, red flags represent events that provide clearer evidence of money laundering or terrorist financing. Below is the list of indicators and red flags that were identified from the analysis of the full cases, though not exhaustive.

INDICATORS

a) Natural and legal persons being sponsored or linking up with PEPs to conduct mining activities;
b) Foreigners holding large amounts of cash, acting as buying and sales agents of exporters in small scale mining area;
c) The signing of bogus contracts in order to divert funds for personal gains;
d) The prevalence of illegal mining and other related activities including the illegal possession of explosives and chemicals used for mining;
e) Locals fronting for foreign nationals to acquire illegal concessions and trading in gold;
f) Foreign and locally organised criminals, purporting to be highly connected, colluding to lure foreign individuals, assuring to give them access to small scale mines,
g) Scammers luring unsuspecting victims particularly foreign nationals into buying fake gold and associating themselves with a financial institution or high public officials;
h) Politically exposed persons involvement and influence in the extractive industry/mining sector;
i) False declaration of mining products (gold and diamonds) for export.

SUSPICIOUS TRANSACTIONS — "RED FLAGS"

a) Buying gold above market price using cash and goods (barter).
b) Making payments for minerals purchased locally to an account abroad.
c) Fund transactions between mining company accounts and Politically Exposed Person (PEP) and/or political party accounts.
d) Purchasing large quantities of gold over and above the market price at small scale mining sites.
e) Comingling legal funds with suspicious proceeds of activities related to precious mineral exploration, mining and/or marketing.
f) Government officials openly involved in unauthorised extraction and trade of minerals.
g) Sudden influx of gold miners into abandoned mining sites.
h) Growing number and influx of foreigners engaged in illegal mining and precious mineral sales.
i) Dealers involved in the sale of gold without licence from the authorities.
j) Lack of links between the principal/legal entity and the beneficiary/natural person;
k) Obscured beneficial ownership.
l) Client indiscriminately purchases merchandise without regard for value, size, or color of precious stones.
m) Purchases or sales that are unusual for client or supplier.
n) Unusual payment methods, such as large amounts of cash, multiple or sequentially numbered money orders, traveler's checks, or cashier's cheques, or payment from third-parties.
o) Attempts by client or supplier to maintain high degree of secrecy with respect to the transaction, such as request that normal business records not be kept.
p) A client orders item, pays for them in cash, cancels the order and then receives a large refund.
q) A client asking about the possibility of returning goods and obtaining a cheque (especially if the client requests that cheque be written to a third party).
r) Purchase appears to be beyond the means of the client based on his stated or known occupation or income.
s) Attempt to use a third party cheque or a third party credit card.
t) Funds from an offshore financial centre rather than a local bank.
u) Transaction lacks a business purpose or has no apparent economic or visible lawful purpose.Purchases or sales that are not in conformity with standard industry practice.
v) Over or under-invoicing, structured, complex, or multiple invoice requests, and high-dollar shipments that are over or underinsured.
w) Unwillingness by a client to provide complete or accurate contact information, financial references or business affiliations.
x) Counterpart presence, such as an affiliated store or branch or associate, in non-cooperative countries and territories or countries that are the subject of advisories issued by the FIC or the FAFT1.

---

[1] More information on which countries these characteristics (i.e., those mentioned in the last bullet) may apply to can be found at the following Web site: http://www.fatf-gafi.org/topics/high-

OTHER UNUSUAL OR SUSPICIOUS ACTIVITIES

a) Employee exhibits a lavish lifestyle that cannot be justified by his/her salary.
b) Employee fails to comply with approved operating guidelines.
c) Employee is reluctant to take a vacation

International typologies for precious metals and stones sector[2]

Retail gold purchases serves as direct method of laundering

A money launderer or someone, acting on their behalf, purchased gold from a retail merchant with funds that were generated directly by an illegal activity. In the case in question, a foreign national used the services of a bureau de change to buy 265 ingots of gold with a total value of about USD 2,440,000, paid in cash. These transactions took place over a period of 18 months. The buyer, who did not have a bank account, alternated temporary jobs with periods of unemployment, suggesting that he was acting on behalf of a third party, whether a natural or legal person, who was probably involved in drug trafficking. The facts were forwarded to the prosecutor, and an investigation was initiated.

Gold purchases facilitate laundering

An asset management company was responsible for managing the bank portfolios of two individuals active in gold purchases in Africa. The purchased African gold was then sold to a gold working company in Country 1, which in turn forwarded its payments to the accounts of the sellers. Debits were regularly made from these accounts to accounts in Country 2. Desiring to verify the use of the funds, the asset management company requested its clients to provide a description of the channels used for making the payments for the gold in Africa. The information received permitted the company to identify an intermediary residing in Europe who was responsible for paying the suppliers in Country 1. The individual in question was described as being closely associated with a corrupt regime in Africa. Based on this information, the asset management company reported the case to the FIU and proceeded to block the accounts. Information exchanged with foreign counterparts permitted the linking of this illegal trade with an ongoing foreign investigation, which targeted the same individual for arms trafficking. The case was transmitted to the office of the public prosecutor which is now working with the foreign authorities to dismantle these operations.

Criminal attempts to launder fraud proceeds through the diamond market

A known criminal who had benefited financially from a fraud that took place outside Country 1 attempted to send money to jewellers. This was with a view to purchasing precious stones. The financial institution holding the account had been concerned about the individual for some time and had made several suspicious transaction reports to the FIU in Country 1. The client attempted

---

riskandnon-cooperativejurisdictions (Information from the Financial Action Task Force about high risk and non-cooperative jurisdictions).

[2] Sources: FATF Report on Money Laundering Typologies 2002-2003 of February 14, 2003

to send USD 8.2 million to the jewellers. Before this took place the bank took the commercial decision to freeze the accounts. The law enforcement agency made initial investigations and was satisfied that the attempt to buy precious stones had been an attempt to launder the proceeds of the fraud.

Diamond trading used as a cover for laundering of illicit funds.

One of the files developed by the FIU of Country 1 relates to a company with its registered office in an offshore centre, whose corporate object was especially broad and which, in particular, encompassed diamond trading. The account that this company held in Country 1 formed the object of numerous international funds transfers in foreign currencies originating in a tax haven. The funds, in very large sums, were then systematically and immediately withdrawn in cash. These withdrawals were made in large denominations of foreign currencies by a third party, who was a director of companies active in diamond trading. In view of the regularity of some of these operations, it was difficult to associate them with any legal commercial activity in the diamond sector, where one would expect the level of the funds generated to fluctuate. From information gathered by the FIU, it appeared that this account was used as a channelling account with the aim of hampering any investigations into the origin and ultimate destination of the funds. This file was passed on for the laundering of funds associated with illicit diamond trafficking and forms the subject of a judicial investigation by the public prosecutor's office.

APPENDIX D – RISK BASED APPROACH
RISK BASED APPROACH – CONTEXT

Reporting Entities are required to conduct an assessment of and document the risks related to ML/TF/PF. A risk-based approach is a process that allows Reporting Entities to identify potential high risks of ML/TF/PF and develop strategies to mitigate them. When it comes to situations where enhanced due diligence is appropriate, a principle of risk-based approach will allow Reporting Entities to focus resources where they are most needed to manage risks within the Reporting Entities tolerance level.

The approach to the management of risk and risk-mitigation requires the leadership and engagement of senior management towards the detection and deterrence of money laundering and terrorist financing. Senior management is ultimately responsible for making management decisions related to policies, procedures and processes that mitigate and control the risks of money laundering and terrorist financing within a business.

The scope of applied measures for prevention and detection of ML/TF/PF should be proportional to the identified ML/TF/PF risk degree (risk-based approach).

There are three steps to establishing a risk based approach: risk assessment, risk mitigation and risk monitoring. The following diagram depicts visually the three different steps in implementing a risk based approach.

Diagram 1: Risk Based Approach

RISK ASSESSMENT - IDENTIFICATION OF SPECIFIC RISK CATEGORIES

The first step of the risk assessment process is to identify the clients, countries or geographic areas; and products, services, transactions or delivery channels unique to the Reporting Entity. Although attempts to launder money, finance terrorism, or conduct other illegal activities through a Reporting Entity can emanate from many different sources, certain clients, countries or geographic areas; type of mineral, volume of transactions or delivery channels may be more vulnerable or have been historically abused by money launderers and criminals. Depending on the specific characteristics of the particular service, or client, the risks are not always the same.

Various factors, such as the number and volume of transactions, geographic locations, and nature of the client relationships, should be considered when the Reporting Entity prepares its risk assessment. The differences in the way a Reporting Entity interacts with the client (face- to-face contact versus electronic transaction) also should be considered. Because of these factors, risks will vary from one Reporting Entity to another.

SERVICE, TRANSACTION OR DELIVERY CHANNEL RISK FACTORS

Certain services offered by the Reporting Entities may pose a higher risk of ML/TF/PF. These services may facilitate a higher degree of anonymity or involve the handling of high volumes of currency or currency equivalents. Some of these services are listed below, but the list is not all inclusive:

a) anonymous transactions (which may include cash).

b) non-face-to-face business relationships or transactions.

c) payment received from unknown or un-associated third parties

d) business conducted by proxy (where someone is representing the client).

CLIENT RISK FACTORS

The DNFBP sector has been categorised as high-risk which requires specific due diligence measures. In addition, Reporting Entities should consider the following client risk factors:

a) the business relationship is conducted in unusual circumstances

b) non-resident clients.

c) clients that have nominee shareholders.

d) businesses that are cash-intensive.

e) the ownership structure of the client appears unusual or excessively complex given the nature of the client's business.

f) PEPs.

g) where the source of funds cannot be determined.

h) where the funds available appears beyond their means.

i) where it is difficult to identify the beneficial owner.

COUNTRY OR GEOGRAPHIC RISK FACTORS

It is essential for Reporting Entity's AML/CFT&P compliance programmes that, they identify geographic locations that may pose a higher risk. Reporting Entities should understand and evaluate the specific risks associated with doing business in, or facilitating transactions involving certain geographic locations. However, geographic risk alone does not necessarily determine a client's or transaction's risk level, either positively or negatively.

INTERNATIONAL HIGHER-RISK GEOGRAPHIC LOCATIONS GENERALLY

This includes:

a) countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML/CFT&P systems including countries listed on the FATF grey or black list.

(https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html)

b) countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations.

c) countries identified by credible sources as having significant levels of corruption or other criminal activity (https://www.transparency.org).

d) countries or geographic areas identified by credible sources as providing funding or support for terrorist activities or that have designated terrorist organisations operating within their country.

Annex A provides a risk assessment checklist to assist Reporting Entities in conducting their ML/TF/PF risk assessment.

ANALYSIS OF SPECIFIC RISK CATEGORIES AND RISK VARIABLES

The second step of the risk assessment process entails a more detailed analysis of the data obtained during the identification stage in order to more accurately assess ML/TF/PF risk. When assessing the money laundering and terrorism financing risks relating to types of clients, countries or geographic areas, type of mineral, volume of transactions or delivery channels risk, a Reporting Entity should take into account risk variables relating to those

risk categories. These variables, either singly or in combination, may increase or decrease the potential risk posed, thus impacting the appropriate level of CDD measures.

Examples of such variables include:

- the purpose of a business transaction or relationship.
- the size of transactions undertaken.
- the regularity or duration of the business relationship.

DEVELOPING THE REPORTING ENTITY'S AML/CFT&P COMPLIANCE PROGRAMME BASED UPON ITS RISK ASSESSMENT

The Management of Reporting Entities should structure their AML/CFT&P compliance programme to adequately address its risk profile, as identified by the risk assessment. Management should understand the Reporting Entity's ML/TF/PF risk exposure and develop the appropriate policies, procedures, and processes to monitor and control ML/TF/PF risks. For example, the Reporting Entity's monitoring systems to identify, research and report suspicious activity should be risk-based, with particular emphasis on higher-risk services, clients, entities, and geographic locations as identified by the Reporting Entity's ML/TF/PF risk assessment.

Internal Auditor/senior official should review the Reporting Entity's risk assessment for reasonableness. Additionally, Management should consider the staffing resources and the level of training necessary to promote adherence with these policies, procedures and processes. For those Reporting Entities that assume a higher-risk ML/TF/PF profile, Management should provide a more robust AML/CFT&P compliance programme that specifically monitors and controls the higher risks that the Board and Management have accepted.

UPDATING REPORTING ENTITY'S RISK ASSESSMENT AND RATING

An effective AML/CFT&P compliance programme controls risks associated with the Reporting Entity's services, clients and geographic locations; therefore, an effective risk assessment should be an ongoing process, not a one-time exercise. Management should update its risk assessment to identify changes in the Reporting Entity's risk profile, as necessary. Even in the absence of such changes, it is a sound practice for Reporting Entity to periodically reassess

their AML/CFT&P risks at least every 12 to 18 months.

RISK PROFILING

Based on the information provided, Reporting Entities should assess the risk profile of their clients taking into consideration the following:

- Evidence of an individual's permanent address sought through an accredited reference agency or through independent verification by home visits;
- Personal reference (i.e. by an existing client of the same Reporting Entity);
- Source(s) of wealth/funds;
- Verification of employment, public position held (where appropriate).

Legal Persons

a) Identification and Verification

For legal persons, the following information should be obtained:

- name of entity;
- principal place of entity's business operations;
- mailing address of the entity;
- contact telephone,
- fax numbers and website address;
- some form of official identification number, if available (e.g. tax identification number, incorporation number);

- the original or certified true copy of the certificate of incorporation and Constitution;
- beneficial owners;
- the resolution of the Board of Directors to transact businesses and identification of those who have authority to act on behalf of the entity;

The Reporting Entity should verify this information by at least one of the following methods:

- for established corporate entities - reviewing a copy of the latest annual report (audited, if available);
- conducting an enquiry by a business information service or an undertaking from a reputable and known firm of lawyers or accountants confirming the documents submitted;
- undertaking a company search to determine its state as to whether the entity has not been or is not in the process of being dissolved, struck off, wound up or terminated;
- utilising an independent information verification process such as accessing public and private databases; and
- contacting the corporate entity by telephone, mail or e-mail.

The reporting entity should also take reasonable steps to verify the identity and reputation of any agent that transacts business on behalf of a corporate client, if that agent is not an officer of the corporate client.

b) Beneficial Ownership

The principal guidance is to look behind the business entity to identify those who own or have control over the business and the entity's assets, including those who have ultimate control.

Particular attention should be paid to shareholders, signatories or others who inject a significant proportion of the capital or financial support or otherwise exercise control. Where the owner is another corporate entity, the objective

is to undertake reasonable measures to look behind that company or entity and to verify the identity of the principals.

What constitutes control for this purpose will depend on the nature of the entity and may rest in those who are mandated to manage the business operations without requiring further authorisation and who would be in a position to override internal procedures and control mechanisms.

Understanding the ownership and control structure of the client and gaining an understanding of the client's source of wealth and source of funds helps reduce the risk of DPMS being abused for ML/TF/PF &PF.

RISK MITIGATION

Risk mitigation is about implementing measures to limit the potential ML/TF/PF risks the Reporting Entity has identified while staying within its risk tolerance level. As part of its internal controls, when the risk assessment determines that risks are high for ML or FT, the dealer has to develop written risk mitigation strategies (policies and procedures designed to mitigate high risk) and apply them for high-risk situations. Annex B provides a list of risk mitigation measures that may be appropriate for situations that you have determined to be higher risk.

It is important that the risk mitigation strategies developed by the Reporting Entity are documented. This allows the risk mitigation strategies to be shared with management and employees. Furthermore, the application of the mitigation strategies should be recorded to demonstrate that mitigation measures have been applied.

RISK MONITORING

In addition to risk assessment and risk mitigation activities, Reporting Entities should also take measures to conduct on-going monitoring of financial transactions. The level of monitoring should be adapted according to the ML/TF/PF risks as outlined in the entity's risk assessment where Reporting Entities review high risk transactions more frequently against suspicious transaction indicators relevant to the relationship and escalate them should additional indicators be detected. The purpose of on-going monitoring activities is to help detect suspicious transactions.

The Reporting Entity's policies, controls and procedures should determine what kind of monitoring is done for particular high-risk situations, including how to detect suspicious transactions. The policies, controls and procedures should also describe when monitoring is done (its frequency), how it is reviewed, and how it will be consistently applied.

With this in mind, Reporting Entities should review transactions based on an approved schedule with specific parameters that involves management sign-off (eg. transactions involving certain countries or over a certain threshold). In conducting this monitoring, Reporting Entities should flag changes in activities that is contrary to normal transaction patterns or client activities. A process should be in place to elevate concerns as necessary.

ANNEX A - RISK ASSESSMENT CHECKLIST

Name of obliged entity: _____

Risk assessment period: _____

The *Anti-Money Laundering Act* requires reporting institutions to conduct a risk assessment of their exposure to ML/TF/PF and apply corresponding mitigation and controls.

This checklist is meant to assist your Entity in meeting these obligations. This form is presented as an example only. You may choose to conduct your risk assessment using a different approach.

Instructions: Review the higher risk clients and situations outlined in the left column and indicate whether you have conducted these activities during the risk assessment period. You should indicate the frequency of each type of transaction in the designated column. When you answer yes to one of the questions, this situation or client is considered higher risk and a control measure to reduce the risk should be applied. For each higher-risk client or situation, a suggested control measure is proposed. You can adapt the control measures to correspond to your business (see Annex B for list of control measures).

When determining the frequency of transactions the Reporting Entity should base its assessment on what is deemed frequent in the context of their own operations and document the rationale.

The results of this risk assessment should be integrated in the Reporting Entities' policies and procedures. In developing policies and procedures that are adapted to the results of the risk assessment findings reporting institutions should take into account the frequency and materiality of higher risk transactions. Your AML/CFT&P focus should prioritize those higher-risk situations that are most frequent and sizable.

This should also include communication to all relevant employees to ensure that they are adequately understood, and control measures implemented. The training of the relevant employees should include a presentation of the risk assessment and the role of employees in the implementation of control measures. You should review your risk assessment

periodically based on changes in legislation or your business activities and at least once a year.

Risk Assessment

Higher risk clients and situations	Yes High frequency of transaction Higher risk	Yes Moderate frequency of transaction Medium-High risk	No transactions Lower risk	Proposed Control Measures
Clients				
Are your clients foreigners?			•	• Determine if individuals are politically exposed persons. • Obtain additional information on source of funds or source of wealth. • Conduct internet search • Increase the frequency of ongoing monitoring
Do you have clients who are politically exposed persons?			•	• Obtain senior management approval to conduct the transaction. • Obtain additional information on source of funds or source of wealth.

Higher risk clients and situations	Yes High frequency of transaction Higher risk	Yes Moderate frequency of transaction Medium-High risk	No transactions Lower risk	Proposed Control Measures
				• Monitor any future transactions.
Is your client an intermediate vehicle such as corporations, trusts, foundations, partnerships or other structure that makes it difficult to determine who is the beneficial owner?				• Obtain name of beneficial owner behind corporation, trust or legal arrangement. • Obtain additional information on organizational structure. • Obtain additional information on source of funds or source of wealth.
Are your clients intermediaries (i.e. lawyers and accountants acting on behalf of clients)?				• Obtain name of person(s) on whose behalf the transaction is being conducted. • Obtain additional information on source of funds or source of wealth.
Has one of your client been named in the media as being involved with criminal organizations?				• File Suspicious Transaction Report (STR). • Obtain additional information on source of funds or source of wealth.
Do you have a client that is conducting a transaction that				• Obtain additional information on source of funds or source of

Higher risk clients and situations	Yes High frequency of transaction Higher risk	Yes Moderate frequency of transaction Medium-High risk	No transactions Lower risk	Proposed Control Measures
is not within his or her means based on his stated occupation or income?				wealth.
Do your clients engage in activities that are consistent with the indicators identified for Suspicious Activities?				• Consider filing a Suspicious Transaction Report (STR). • Obtain additional information on source of funds or source of wealth.
Geographic Risk				
Do you sell any precious metals or stones that is considered higher risk in the precious metals and stones supply chain?				• Obtain senior management approval to proceed with the transaction. • Obtain additional information concerning the orgins of the precious metals and precious stones • Increase the frequency of ongoing monitoring
Are any of your clients or the source funds originate from countries subject to sanctions, embargoes or similar				• Obtain senior management approval to proceed with the transaction. • Ask for additional piece of

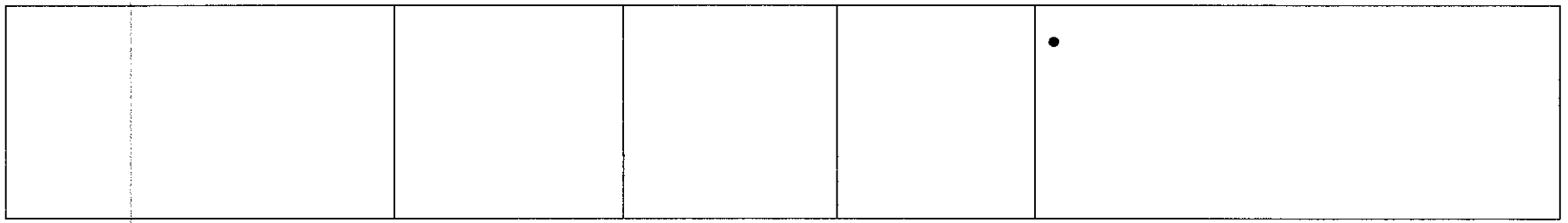
Higher risk clients and situations	Yes High frequency of transaction Higher risk	Yes Moderate frequency of transaction Medium-High risk	No transactions Lower risk	Proposed Control Measures
measures issued by Uganda or International Organizations such as the United Nations ("UN"). United Nations: https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list				identification to confirm the identity. • Obtain additional information on source of funds or source of wealth. • Increase the frequency of ongoing monitoring
Are any of your clients or the source funds originate from countries identified as financial secrecy havens or jurisdictions.				• Obtain senior management approval to proceed with the transaction. • Ask for an additional piece of identification to confirm the identity. • Obtain additional information on source of funds or source of wealth. • Increase the frequency of ongoing monitoring
• Are any of your clients or the source funds originate				• Obtain senior management approval to proceed with the

Higher risk clients and situations	Yes High frequency of transaction Higher risk	Yes Moderate frequency of transaction Medium-High risk	No transactions Lower risk	Proposed Control Measures
from countries identified by the Financial Action Task Force (FATF) as having strategic deficiencies in the fight against money laundering or subject to an FATF statement? https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html				transaction. • Ask for an additional piece of identification to confirm the identity. • Obtain additional information on source of funds or source of wealth. • Increase the frequency of ongoing monitoring
• Are any of your clients or the source funds originate from countries identified by credible sources as providing funding or support for terrorist activities?				• Obtain senior management approval to proceed with the transaction. • Ask for an additional piece of identification to confirm the identity. • Obtain additional information on source of funds or source of wealth. • Increase the frequency of ongoing monitoring
• Are any of your clients or the source funds originate				• Obtain senior management approval to proceed with the

Higher risk clients and situations	Yes High frequency of transaction Higher risk	Yes Moderate frequency of transaction Medium-High risk	No transactions Lower risk	Proposed Control Measures
from countries identified by credible sources as having significant levels of corruption, or other criminal activity? https://www.transparency.org/en/publications				transaction. • Ask for an additional piece of identification to confirm the identity. • Obtain additional information on source of funds or source of wealth. • Conduct additional research on the client.

Delivery channel and business practices				
Do you accept cash?				• Confirm source of funds • Set limits to cash transaction amounts. • Request bank drafts instead of accepting large amounts of cash.
Do you conduct transactions where you do not meet the client?				• Deliver comprehensive AML/CFT&P training specifically focused on client due diligence requirements • Ask for an additional piece of identification to confirm the identity. • Conduct periodic review of records to ensure that client due diligence requirements are adequately implemented
Do you have clients that are referred to you by a third party?				• Conduct client due diligence measures directly. • Conduct periodic review of records to ensure that client due diligence requirements are respected by third party.
Do you have short-term or part-time agents?				• Include ML/FT obligations in job descriptions and performance reviews. • Deliver comprehensive AML/CFT&P training for all agents

Do you undertake high value transactions?				• Pay special attention for unusual transaction and ML/TF/PF indicators. • Obtain additional information on source of funds or source of wealth. • Increase the frequency of ongoing monitoring
Other risk factors: (list any additional factors)				
				•
Other factors: **Obliged entities should list products/services that are deemed high risk in their sector as determined by their risk analysis or the national risk assessment**				
				•



Specific risk factors for dealers in precious metals and stones				
Higher risk clients and situations	**Yes** **High frequency of transaction** **Higher risk**	**Yes** **Moderate frequency of transaction** **Moderate risk**	**No transactions** **Lower risk**	**Proposed Control Measures**
Import of precious metals and stones from higher risk jurisdictions				• Document information on the origins of the precious metals/precious stones • Pay special attention for unusual transaction and ML/TF/PF indicators. • Obtain additional identification document on seller • Conduct an internet search on seller
Export of precious metals and stones from higher risk jurisdictions				• Document information on the origins of the precious metals/precious stones • Pay special attention for unusual transaction and ML/TF/PF

				indicators. • Obtain additional identification documents on buyer • Obtain information on source of funds • Conduct an internet search on buyer
Wholesale of precious metals and stones from higher jurisdictions				• Document information on the origins of the precious metals/precious stones • Pay special attention for unusual transaction and ML/TF/PF indicators.
Retail sale of precious metals and stones – high value sales[3]				• Obtain additional information on source of funds. • Pay special attention for unusual transaction and ML/TF/PF indicators.
Manufacturing of jewellery				• Pay special attention for unusual transaction and ML/TF/PF indicators. • Document information on the origins of the precious metals/precious stones

Selling of loose stones (diamonds, etc)				• Pay special attention for unusual transaction and ML/TF/PF indicators. • Determine if buyer is affiliated with a high risk jurisdiction • Conduct an internet search on buyer
Sale of gold bars and coins				• Pay special attention for unusual transaction and ML/TF/PF indicators. • Determine if buyer is affiliated with a high risk jurisdiction • Conduct an internet search on buyer
Purchase or sale of precious metals and precious stones where terrorist organisations are operating				• Pay special attention for unusual transaction and ML/TF/PF indicators. • Determine if buyer may be affiliated with a terrorist organisation • Conduct an internet search on buyer

_____

_____

Signature of the AMLRO ***Date***

Date of employee training: _____

ANNEX B - RISK MITIGATION MEASURES

Risk mitigation measures for high risk situations may include:

i. increased awareness of higher risk situations within business lines across the entity;
ii. increased monitoring of transactions;
iii. the approval of the establishment of relationships is escalated to senior management;
iv. the levels of on-going controls and reviews of relationships are increased;
v. personnel that have clear lines of authority, responsibility and accountability;
vi. adequate segregation of duties (for example, an employee establishing a relationship with a client is not authorized to also approve it as that authorization is the responsibility of someone else in the organization);
vii. proper procedures for authorization (for example, an employee processing a transaction for which the amount exceeds a certain threshold has to follow a procedure to get approval for the transaction by someone else in the organization);
viii. internal reviews to validate the risk assessment processes;
ix. seeking additional information beyond the minimum requirements to substantiate the client's identity or the beneficial ownership of an entity;
x. obtaining additional information about the intended nature of the relationship, including estimates regarding the amount and type of business activity;
xi. obtaining additional documented information regarding the client' source of funds and accumulation of wealth;
xii. requesting high risk clients to provide additional, documented information regarding controls they have implemented to safeguard their operations from abuse by money launderers and terrorists;
xiii. getting independent verification of information (i.e. from a credible source other than the client);
xiv. stopping any transaction with a potential client until identification information has been obtained;
xv. implementing an appropriate process to approve all relationships identified as high risk as part of the client acceptance process or declining to do business with potential clients because they exceed your risk tolerance level;
xvi. implementing a process to exit from an existing high risk relationship which is beyond the entity's stated risk tolerance level; and
xvii. analysing money laundering and terrorist financing risk vulnerabilities for new acquisition processes and for product or service development processes.

APPENDIX E - SUBMISSION OF STATUTORY RETURNS

TYPE OF REPORT	RECIPIENT BODY	CHANNEL	FREQUENCY
Compliance Report This shall include but not limited to the following keys areas **1. Employees AML/CFT&P Training Conducted** **2. Additional Procedures and Mitigants** **3. New Technologies (eg. crypto currency transactions), Non-face-to-face Transactions** **4. Reliance on Intermediaries or Third-Party Service Providers** **5. Update on appointment / redesignation / dismissal /resignation for AMLRO** **6. Monitoring of Employee Conduct (eg. lifestyle)** **7. Fraud activities** **8. Review of Risk Assessment Conducted** **9. Review of AML/CFT&P policy/framework** **10. Record Keeping Procedures**	MINCOM & FIC	To MINCOM through aml@mincom.gov.gh To FIC via info@fic.gov.gh and compliancemails@fic.gov.gh	**HALF YEARLY** (not later than the 15th day of the month after the half year); and **END OF YEAR** (not later than the 15th day of the month after the end of year)

11. Statistics of STRs and CTRs submitted to the FIC during the review period **12. Other relevant compliance Activities**			
Employee Education & Training Programme/Plan	MINCOM & FIC	To MINCOM through aml@mincom.gov.gh To FIC via info@fic.gov.gh and compliancemails@fic.gov.gh	**YEARLY** (not later than 31st December of every financial year)
Independent Audit Report on AML/CFT&P Compliance Function The report may include but not limited to the following areas: **1. Review of AML/CFT&P programme for the year** **2. Review of Board/employees training** **3. Review of AML/CFT&P policy & Risk Assessment Framework** **4. Review of CTRs/STRs filed** **5. Review of KYC/CDD/EDD on customers** **6. Review of due diligence on new employees**	MINCOM & FIC	To MINCOM through aml@mincom.gov.gh To FIC via info@fic.gov.gh and compliancemails@fic.gov.gh	**YEARLY** (not later than the 15th February of the ensuing year)

7. Review of any other AML/CFT&P related activity			
Filing of STRs	FIC	GOAML	**As and When**
Filing of CTRs	FIC	GOAML	**Daily**
Submission of updated PEP List	FIC	info@fic.gov.gh and compliancemails@fic.gov.gh	**QUARTERLY** (not later than the 15th day of the month after the end of the quarter)
Submission of PEP Transactions	FIC	GoAML	As and When
Completion of Statistical Questionnaire (Appendix A)	Mincom	To MINCOM through aml@mincom.gov.gh	Annually By 30th January of the ensuing year