Ghana Infrastructure Investment Fund
Anti-Money Laundering (AML) & Counter-Terrorism Financing (CFT) Policy

As approved by the Board of Directors on 27th July, 2026

Contents

1.0 Introduction

Ghana Infrastructure Investment Fund (GIIF) has set out this policy that is applicable to all staff to help prevent and detect potential money laundering or terrorist financing activity. The Company takes a zero-tolerance approach to money laundering, terrorist activity and other such financial crimes.

1.2 The Company will ensure it has appropriate policies and procedures in place to complement this AML policy, in compliance with applicable regulations, and monitoring of adherence to those policies will also take place.

1.3 All staff will be trained in AML/CFT processes and procedures for the Company and will actively participate in preventing the services of the Company from being exploited by criminals and terrorists for money laundering or terrorist financing purposes. The objectives of this and related policies are:

- ensuring the Company's compliance with all applicable laws, statutory instruments of regulation, and requirements both locally and internationally;
- protecting the Company and its staff as individuals from the risks associated with breaches of the law and regulations
- preserving the good name of the Company against the risk of reputational damage presented by implication in money laundering and terrorist financing activities;
- • making a positive contribution to the fight against crime and terrorism.

1.4 To achieve these objectives, it is the policy of this Company that:

- every member of staff shall meet their personal obligations as appropriate to their role and position in the Company
- neither commercial considerations nor a sense of loyalty to clients or sponsors shall be permitted to take precedence over the Company's anti-money laundering commitment
- the Company shall appoint a Money Laundering Reporting Officer (MLRO) and they shall be afforded every assistance and cooperation by all members of staff in carrying out the duties of their appointment;
- the Company shall have anti-money laundering policies and procedures outlining the positive actions to be taken by staff during their work, and the MLRO shall keep these under review to ensure their continuing appropriateness.

1.5 Failure to comply with the AML and associated policies could result in disciplinary proceedings which could ultimately lead to dismissal.

2.0 Key AML Concepts

This section summarizes key AML compliance concepts and definitions.

2.1 Money Laundering

GIIF's Anti Money Laundering Policy shall be in compliance with Ghana's 2020 AML Policy Act 1044 which defines Money Laundering as follows

A person commits money laundering when a person knows or ought to have known that a property is, or form part of, the proceeds of an unlawful activity and the person:

- Converts, conceals, disguises, or transfers the property for the purpose of
  - **a.** concealing or disguising the illicit origin of the property or
  - **b.** assisting any person who is involved in the commission of the unlawful activity to evade the legal consequences of the unlawful activity.
  - **c.** Conceals or disguises the true nature, source, location, disposition, movement or ownership, or right to, the property; or
  - **d.** Acquires, uses or takes possession knowing or suspecting at the time of receipt, that the property is or forms part of the proceeds of unlawful activity
  - **e.** Where a person under investigation for money laundering is in possession of control of property which the person cannot account for and which is disproportionate to the income of that person from known sources, that person shall be deemed to have committed an offence.

Money Laundering is the process by which criminals attempt to conceal the true origin and ownership of the proceeds of illegal activities. The phrase 'money laundering' covers all methods used to change the identity of illegally obtained money so that it can be used for legitimate purposes.

Money laundering is not restricted to the proceeds of drug trafficking. It includes proceeds from other criminal activities such as armed robbery, tax evasion, smuggling, prostitution, terrorism, arms dealing, fraud, forgery and counterfeiting, bribery and corruption.

Money laundering is a major threat to financial institutions and the economic stability of entire countries. Governments worldwide have introduced legislation to prevent it, including specific money laundering offences and legally imposed requirements on institutions operating in their jurisdictions.

2.1.1 The Money Laundering Process

The main objective of the money launderer is to transform ‘dirty’ money into seemingly clean money or other assets in a way to leave as little trace as possible of the transformation.

There are essentially three recognized forms of the money laundering process:

(a) Placement

For criminals this is the most vulnerable step in the ‘washing’ cycle. This is the physical immersion of the criminally derived funds into the financial system. Examples: Use cash to buy a bank draft to pay into a bank account. Transfer cash to another country by wire transfer. Use the cash to buy traveler’s cheques or foreign exchange. Buying a house, car, antiques etc.

(b) Layering

The purpose of layering is to disassociate the illegal monies from the source and perpetrator of the crime by purposely creating a complex web of financial transactions aimed at concealing any audit trail.

Examples: Send the money by wire transfer to other countries, to different people, to a variety of accounts in a variety of currencies. Buy shares, which can be sold. Transfer money to an offshore account.

(c) Integration

The stage at which the money is integrated into the legitimate economic and financial system and is assimilated with all the other assets in the system. At this stage it becomes virtually impossible to distinguish between ‘respectable’ and ‘dirty’ money.

Examples: Purchase of fast-food outlets or other cash intensive businesses/properties or possibly investing a in project as an equity contributor with the money and approaching GIIF to provide additional capital to complete a project.

In basic terms, the money launderer wants to:

Place money in the financial system, without arousing suspicion.

Move money around, often in a series of complex transactions crossing multiple jurisdictions, so it becomes difficult to identify its original source, and then Move the money back into the financial and business system, so that it appears as legitimate funds or assets.

The physical disposal of cash, which starts to break the link with the original crime by placing money back into the economy.

The criminal tries to pass the money through as many layers as possible.

Successful layering results in the money being returned to the economy in what appears to be legitimate business funds.

2.1.2 Methods of Money Laundering

There are as many methods to launder money as the imagination allows, and the schemes being used are becoming increasingly sophisticated and complicated as technology advances. The following are some examples of common money laundering methods.

- Nominees

  This is one of the most common methods of laundering and hiding assets. A launderer uses family members, friends or associates who are trusted within the community, and who will not attract attention, to conduct transactions on their behalf. The use of nominees facilitates the concealment of the source and ownership of the funds involved.

- Structuring or “smurfing”

  Many inconspicuous individuals deposit cash or buy bank drafts at various institutions, or one individual carries out transactions for amounts less than the amount that must be reported to the government, and the cash is subsequently transferred to a central account. These individuals commonly referred to as “smurfs,” normally do not attract attention as they deal in funds that are below reporting thresholds and they appear to be conducting ordinary transactions.

- Asset purchases with bulk cash

  Individuals purchase big-ticket items such as cars, boats and real estate. In many cases, launderers use the assets but distance themselves from them by having them registered in a friend or relative’s name. The assets may also be resold to further launder the proceeds.

- Exchange transactions

  Individuals often use proceeds of crime to buy foreign currency that can then be transferred to offshore bank accounts anywhere in the world or converted in foreign currency drafts/travelers cheques.

- Currency smuggling

  Funds are moved across borders to disguise their source and ownership and to avoid being exposed to the law and systems that record money entering into the financial system. Funds are smuggled in various ways (such as by mail, courier and body-packing) often to countries with strict bank secrecy laws.

- Gambling in casinos

  Individuals bring cash to a casino and buy gambling chips. After gaming and placing just a few bets, the gambler redeems the remainder of the chips and requests a casino cheque.

- Black-market peso exchange

  An underground network of currency brokers with offices in North America, the Caribbean and South America allows drug traffickers to exchange pesos for U.S. dollars. The dollars stay in the United States and are bought by South American (mainly Colombian) companies, which use them to buy American goods for sale back home.

- Hawalas/ Hundi/ Chit (Informal money transfer businesses)

  Informal networks that move money on a trust- based pact, with next to no record keeping or formal paper trails. Usually family/clan based front companies/ businesses and is popular with cultures that do not use or trust formal banking. Pre-Dates any formal banking systems and moves millions of dollars globally.

2.1.3 Worldwide Legislation

A major result of international concerns about the extent of money laundering was the creation of the Financial Action Task Force (FATF). The FATF is a body whose purpose is to examine worldwide compliance to existing money laundering legislation and to recommend additional requirements where appropriate.

The FATF has representatives from over 30 countries and two international organizations. Its membership includes the major financial centres of Europe, North and South America, and Asia. It is a multidisciplinary body bringing together the policymaking power of legal, financial and law enforcement experts.

The FATF made recommendations to raise the international standards of money laundering compliance to a uniform level. These recommendations set out the basic framework for money laundering prevention efforts and are designed to be of universal application. It was recognized from the outset of FATF, that countries have diverse legal and financial systems. The recommendations are therefore the principles for action for countries to implement according to their particular circumstances, allowing countries a measure of flexibility rather than prescribing every detail.

FATF continually inspect and assess the level of anti-money laundering compliance in countries around the globe. Those governments who fail to provide an adequate anti-money laundering framework damage their opportunities for international trade.

It can be an offence for employees within Ghana Infrastructure Investment Fund (GIIF) to:

- *knowingly assist in concealing or otherwise dealing in criminal property and/or criminal proceeds;*
- *fail to report knowledge or suspicion that another person is engaged in money laundering;*
- *fail to report where there are reasonable grounds for knowing or suspecting that another person is engaged in money laundering; and*
- *"Tip off" another person that a report has been made or disclose that an investigation has commenced.*

2.2 Terrorist Financing

Terrorist financing may occur through methods that are similar to money laundering.

However, it is important to note characteristics of terrorist financing that can make it even more difficult to detect than money laundering:

- terrorists may finance attacks through simple transactions that involve a relatively small amount of money and may be indistinguishable from normal activity;
- terrorists may finance attacks using both unlawful and lawful sources of funds, including charitable donations, unlike money laundering where the source of funds is always unlawful; and
- In terrorist financing, the focus is primarily on the usage of the funds, whether lawfully or unlawfully derived.

In addition to these characteristics, it can be hard to recognize terrorist financing because financial institutions often see only a small portion of a sponsor's/Client's overall activity. Because terrorist financing can be so difficult to identify, it is especially important for Employees to report any suspicions they may have in dealing with these clients/sponsors or promoters of projects submitted to the fund for financing.

2.3 Willful Blindness and Evasion

In Ghana, it is an offence if institutions and their Employees may be found to violate AML compliance requirements if they acted with "willful blindness." Willful blindness" means "turning a blind eye" or "consciously avoiding" facts or suspicions of money laundering or terrorist financing.

It is also a crime to structure transactions in order to evade AML reporting requirements.

3.0 Compliance Programme

Ghana Infrastructure Investment Fund (GIIF) must maintain an AML programme consisting of a minimum of:

- A designated Compliance Officer working closely with the Risk Manager
- An annual risk assessment;
- Risk-based controls;
- Transaction Monitoring
- Employee AML training and awareness;
- Independent testing (internal/external Audits);
- Ongoing reporting to senior management, including provision of meaningful and accurate Management Information to the CEO
- Compliance with local AML laws and regulation where the standard is higher than this Policy.

In addition, it is specifically forbidden for any Employee to circumvent this Policy or advise anyone on how to circumvent this Policy.

Compliance Manager

GIIF shall have in place a Compliance Officer/Manager with experience, stature, and authority commensurate with the AML risks the business faces. The Compliance Manager must be independent of line of business management.

The Compliance Manager's responsibilities shall include;

- Developing an AML/CFT Compliance Programme;
- Receiving and vetting suspicious transaction reports from staff;
- Filing suspicious transaction report with the Financial Intelligence Center (FIC);
- Ensuring that the Institution's compliance programme is implemented;
- Co-ordinating the training of staff in AML/CFT awareness, detection methods and reporting requirements;

The Compliance Manager shall be nominated/recruited by the CEO with the approval of the Board of Directors.

3.1 Risk Assessment

The MLRO shall put in place a risk assessment mechanism that would facilitate appropriate identification, management, monitoring and control of the following:

a) The level of money laundering risk inherent in all activities undertaken across the business (i.e. internal and external).

b) The level of controls through which all parts of the business (both internal and external) manage this risk.

The methodology must consider the following risk factors including, at a minimum:

- Nature, scale, and complexity of the business, including its processes and operations, as well as volume and size of transactions;
- diversity of operations, including geographical diversity and the risks that arise from exposure to different geographies;
- Client/Sponsor characteristics;
- products and services; and

Compliance Officer is responsible for executing the risk assessment and obtaining the agreement of senior management of the various departments and acknowledgement from the CEO. Where a risk assessment identifies gaps within controls or a requirement for new controls, an Action Plan to address any gaps must be devised by the Compliance Officer.

Combined Risk Framework (CRF)

The Combined Risk Framework (CRF) is a risk profiling template that determines the risk level of a sponsor. It should be completed prior to acceptance of project into GIIFs pipeline and investment team starts any process towards appraisal of the project.

3.2 Risk-Based Controls

The Compliance Officer/AMLRO must ensure that risk-based controls are in place, including policies and/or procedures that are:

- reasonably designed to deter, detect and report known or suspected money laundering and terrorist financing; and
- Consistent with this Policy.

  The controls must be comprehensive and proportionate to the nature and scale of business activities.

3.3 Training and Awareness

The Compliance Officer/AMLRO must ensure AML compliance training is provided, at a minimum on an annual basis, to all relevant employees, including senior management.

The AMLRO must determine which employees are “relevant” and what the appropriate training is. He/she should ensure that, through the Human Resources department’s processes or otherwise, employees that move between departments still continue to receive AML training at appropriate frequencies and levels.

The Compliance Officer/AMLRO should consider at least the following types of Employees as "relevant":

- Investment team;
- Risk Department
- Human Resource/Legal; and
- Senior management.

The Compliance function must ensure that the training curriculum is current and relevant to GIIFs operations. The following Training modules must be rolled out in creating awareness on the policies annually for all staff: Code of Conduct, AML/CFT, and Anti Bribery & Corruption. Compliance function must roll out reviewed and agreed upon Policies for the discussion and training of all staff.

3.4 Independent Testing

Compliance with this Policy is subject to independent periodic testing by the Internal Audit and reports the results to the Compliance Officer and the CEO, or as per the applicable GIIF Internal Control governance and reporting process.

There could also be reviews or audits from the Auditor General or it's appointed entity/representative.

3.5 Conformance

The various departments and potential sub-funds must take steps to assess their conformance (through compliance monitoring/quality assurance) with this Policy through periodic testing to assess the effectiveness of their systems and controls. Departments and other Sub-Funds must remediate promptly any non-conformance or ineffective systems and controls identified. Instances of non-conformance must be reported as a breach without delay and an Action Plan devised and tracked to completion, keeping the CEO up to date.

In the event the requirements of this Policy cannot be met by any of the departments, one of the following requests must be submitted to the Compliance Manager:

- a Dispensation request;
- a Waiver request; or
- A Breach notification.

The various departments must use the appropriate forms to request for any Dispensations/Deferrals or Waivers and to report any Breaches.

A detailed Action Plan will typically be required to support requests for Dispensation/Deferrals and Notifications of Breaches. Each Action Plan should include an overview of the proposed actions, both tactical and strategic, that will deliver Policy conformance.

Please refer to the Action Plan section within the Dispensation/Deferrals and Breach forms for further details.

3.5.1. Dispensations/Deferrals

A Dispensation/Deferral is a request for temporary exemption from a specific requirement of this Policy. All Dispensation/Deferral requests should be supported by a detailed Action Plan. * Refer to the appendices of the Standard guidelines on AML/CFT for the form.

3.5.2. Waivers

A Waiver is a request for long-term exemption from a specific requirement of this Policy and must be subject to regular review (at least annually) by the Compliance Manager. A Waiver should only be sought in cases where a department seeks a permanent exemption from compliance with a requirement(s) of this Policy. A Waiver cannot be sought against an applicable legal/regulatory requirement. Where local law/regulation prevents full application of the Policy requirements, a Waiver must be sought.

3.5.3 Breaches

A Breach is deemed to have occurred if a Department/Sub-Fund identifies a Policy requirement that has not been met and is not covered by an approved Dispensation or Waiver.

Departments/Sub-Funds should report any Breaches of this Policy to the Compliance Officer. This includes, but is not limited to,

Breaches discovered through:

- Conformance testing;
- Internal Control audits - for ‘High’ priority observations against a specific requirement within this Policy; and
- Key Indicator (KI) metrics.

3.6 Reporting

Compliance Officer must provide ongoing reporting to senior management, including provision of meaningful and accurate Management Information to the CEO.

3.7 Compliance with Local Laws and AML Regulations

Where a Business Unit/Subsidiary/Sub-fund operates in a jurisdiction with corresponding standards of a higher level than those within this Policy, such local laws and regulations must be followed.

Where there is a conflict between the requirements of this Policy and local law/regulations, advice must be sought from the Compliance Manager.

4.0 Sponsor/Client/Customer Due Diligence and Ongoing Monitoring

To identify potential criminal activity and protect the institution, relevant Client/Sponsor in conjunction with the Client's/Sponsor's activity seen within the relationship. This includes:

- The Sponsor/Client/Customer take-on process; i.e. where relationship is yet to be firmed up
- Ongoing updates of CDD; and
- Ongoing monitoring of Client/Sponsor activity.

4.1 CDD at Take-on

Sponsor/Client/Customer Due Diligence (CDD) occurs at Client/Customer take- on and includes:

- Identification (taking the identity information from the Client/Customer such as name and address);
- Verification (using reliable sources, including documentation, to verify the identity information provided);
- understanding the control and ultimate ownership of Clients/Customers that are Entities and where required, verifying relevant controllers and Ultimate Beneficial Owners and
- Identifying any Politically Exposed Persons (PEPs).

Client/Customer take-on, will in certain circumstances involve:

- Enhanced Due Diligence (EDD);

- Simplified Due Diligence (SDD);
- exceptions from CDD;
- Client/Sponsor categorization and approval of PEPs and High Risk Customers; and/or

This information must be updated at regular intervals or on trigger events.

4.1.1 Identification/Screening

Identification is the taking of identity information from the Sponsor/Client in accordance with the applicable KYC Minimum Standard.

Identification must be performed before entering into a relationship with a new sponsor of any project submitted to the fund for financing. It is recognized that the Client/sponsor identification requirements at take-on may differ over time and as such the standards for remediation of Client/sponsor identification requirements and those required at take-on may differ.

Screening at this time of the institution's development (subject to review) will be done manually by downloading the various sanctions list such as UN, OFAC, UK, France sanctions lists and the lists below and screening the name of subject against it. This will be done by the Compliance Manager when on-boarding a facility. At a later time however, software will be procured to undertake this.

a. European Union Sanctions Lists
We basically reference the EU consolidated financial sanctions lists, which includes persons, groups, and entities subject to EU restrictive measures
Link: https://webgate.ec.europa.eu/fsd/fsf/
b. Office of Foreign Assets Control (OFAC) -U.S Department of the treasury Specially designated nationals (SDN) and blocked persons lists
Link: https://sanctionssearch.ofac.treas.gov/
c. Financial Action Task Force (FATF) High-Risk Jurisdictions and Jurisdictions under increased monitoring
Link: https://www.fatf-gafi.org/
d. World Bank and Other MDB Debarment Lists (where applicable during due diligence reviews). World Bank Listing of Ineligible Firms and Individuals:
Link: https://www.worldbank.org/en/projects-operations/procurement/debarred-firms
e. United Nations Security Council (UNSC) Sanctions List
Link: https://www.un.org/securitycouncil/sanctions/information
f. UK Sanctions List (OFSI/UK Govt)
https://www.gov.uk/government/publications/the-uk-sanctions-list
g. United Kingdom Sanctions List (OFSI / UK Government)
Link: https://www.gov.uk/government/publications/the-uk-sanctions-list

4.1.2 Verification

Verification is the use of reliable sources to verify the identity information provided by the Client/Sponsor.

The investment team and all other business units/sub-funds created either in Ghana or abroad may determine the method of verification on the basis of local requirements, their risk assessment, and available verification documents and data sources provided these meet the company's KYC Minimum Standard and any applicable business unit level guidance.

4.1.4 Controllers and Ultimate Beneficial Owners

Entities can be used to conceal money laundering activities. It is therefore important to ensure that controllers and Ultimate Beneficial Owner of Entities are identified and verified. For Entities listed on Stock Exchanges, regulation and best practice allows Simplified Due Diligence (SDD). For other Entities, for example private companies, due diligence on controllers and Ultimate Beneficial Owners (UBOs) must be performed.

Where required, the department (in this case mostly Investment department) must take measures to reach an understanding of the Client's/Sponsor's control and ownership structure by considering information such as:

- the legal form of the Entity (e.g. corporation, limited company, partnership, trust, etc.) and;
- The controllers of the company (e.g. a general understanding of who within the Entity is authorized to make major decisions, such as executive management or executors).

The Departments must verify the identity of controllers and Ultimate Beneficial Owners according to GIIFs risk-based approach.

Individual exceptions to this requirement can be granted exclusively by the Compliance Manager upon documented escalation and clearly recorded risk-based consideration. Exceptions relating to whole categories of Client/Sponsor, rather than individual exceptions, should be clearly documented in a risk assessment otherwise a waiver would be required.

At client take-on, a higher standard of due diligence must be applied to controllers and Ultimate Beneficial Owners of those entities which are high risk according to company Policy.

In instances where GIIF is not able to conduct satisfactory KYC due diligence on an Ultimate Beneficiary Owner (e.g. GIIF is not able to identify and verify UBO, understand ownership or controlling structure) business relationship will stop and forbid any transaction.

4.1.5 Politically Exposed Persons

Political exposure in its own right does not equate to bribery and corruption but may heighten the risk of it. The risks of Politically Exposed Persons (PEPs) are that they may handle proceeds of corruption and/or expect/demand bribes. Equally, the risk of bribery and corruption is not limited to PEPs.

When taking on new sponsors/clients and updating existing CDD, client's must be screened against publicly available PEPs lists in order to determine whether Clients/Sponsor's are politically exposed. Screening of existing Clients/sponsors can be risk-based and performed periodically. Any investigations must be completed within 30 days.

GIIF must, as a minimum, screen all client/sponsor relationships on at least a half yearly basis to identify any individual who may have subsequently become a PEP or closely related to a PEP.

PEP status of a Client/Sponsor should be a factor considered when categorizing the overall Client/Sponsor/Project risk. When an Ultimate Beneficial Owner or Controller of an Entity is PEP, this automatically requires categorization of that client as high risk.

It is recognized that in some circumstances, certain sponsors may be designated as PEPs where there are no clear grounds for such a designation. The Compliance Manager may discount these listings but when doing so the reasoning must be clearly recorded.

For any Client/Sponsor identified as a PEP, Enhanced Due Diligence and appropriate escalation and approval processes must be followed.

Examples of PEPs

- Heads of State or government – President and Vice - current and past
- Ministers of State – current and past
- Members of Parliament – current and past

- High ranking political party officials
- An artificial politically exposed person (an unnatural legal entity belonging to a PEP e.g. companies/corporations)
- Political Parties
- Senior Public Officials- Chief Directors of Civil and Public service
- Senior Judicial Officials- High Court Judges and above
- Senior Military Officials
- Senior Police Officers- Commissioners and above
- Chief Executives of State owned companies/corporations
- Paramount Chiefs
- Family members or close associates of PEPs
- Priests or Imams usually involved in national affairs

4.1.6 Enhanced Due Diligence

The institution will perform Enhanced Due Diligence (EDD), on a risk-sensitive basis, during take-on where the Client/Sponsor represents a higher risk of money laundering or terrorist financing.

There are three specific types of relationship where EDD must be applied, namely:

- Where the Client/Sponsor is not physically present for identification purposes;
- Non-resident foreigner; or
- Where a business relationship or occasional transaction involves a PEP.

Further consideration should be given to performing EDD in other higher risk situations, including but not limited to where the client:

- resides, operates or is incorporated in a high risk country;
- is from a high risk industry (see table 1.0 below);
- Has businesses/products that may present a greater risk of money laundering, terrorist financing or proliferation financing.
- Has other risk factors as defined by GIIF.

The EDD must be recorded. EDD may lead to a conclusion that the given Client/Sponsor does not ultimately pose high risk to the business, i.e., EDD may not lead directly to the high risk categorization of a Client/Sponsor. If so, business unit - specific procedures must clearly define the related categorization process.

Examples of high risk industries

- Money Service Businesses (MSBs);
- Bureau de change businesses.
- Casinos and other forms of gaming/gambling operations, including internet gambling.

See FATF Casino and Gaming sector AML vulnerabilities report. http://www.fatfgafi. org/dataoecd/47/49/42458373.pdf. See also FATF risk based approach. http://www.fatfgafi.org/searchResult/0,3400,en_32250379_3223572 0_1_1_1_1_1, 00.html (search for "casino")

- Businesses involved in the production of arms or military products/equipment.
- Dealer in high-value goods. E.g. Jewelers, Antique Dealers etc.
- Charities, church bodies/places of worship and nonprofit organizations (NPOs), e.g. in circumstances where it is considered that there may be a heightened risk of abuse or exploitation for money laundering or terrorist financing purposes. Possible indicators of heightened risk includes, but are not limited to
  - Close alignment to particular religious or cultural movements;
  - Frequent movements of funds or other resources to areas of conflict around the world;
  - Funds being passed to other organizations based in a different jurisdiction rather than being delivered directly;
  - Dealing exclusively in cash or alternative remittance systems;
  - Having extremely complex financial records in which suspicious transactions are less easy to identify.

Note: this is not an exhaustive list; GIIF may add other industries as appropriate.

4.1.7 Simplified Due Diligence

Provided a Client/sponsor has been identified as low risk by the appropriate department of Business Unit/Sub-Fund, there are a number of limited circumstances (listed below) where Simplified Due Diligence (SDD) may be applied.

Specifically, SDD may be applied to the following entity types, products and individuals:

- entities listed on Stock Exchange;
- Ultimate Beneficial Owners of pooled accounts held by notaries or independent legal professionals;

- Public Authorities (Government Institutions, Ministries, Metropolitan, Municipal Authorities etc);
- Community institutions;

  The application of SDD in the above scenarios gives rise to instances where it may not be necessary to:
- Verify the Client's/Sponsor's / Ultimate Beneficial Owner's identity; or
- Obtain the Ultimate Beneficial Owner's information where a Client/Sponsor is an entity.

  The following minimum information should be obtained when applying SDD to an Entity:
- Full name of the Entity; and

  An Individual:
- Full name of the individual.

Additional information such as address, or country of citizenship should be obtained and / or verified in accordance with GIIFs requirements. The level of verification required shall be determined according to GIIFs risk-based approach.

4.1.8 Reliance on CDD from other Sub-Funds operated by GIIF

Subject to local regulatory requirements, Sub-Funds can rely on the CDD performed by another Unit within the institution provided:

- The existing KYC or CDD is sufficient for the purposes of the new relationship;
- The existing KYC can be readily accessed;
- There are appropriate arrangements for record retention within the Sub-Fund/Unit that is being relied upon.

The receiving Sub-Fund/Unit must determine the appropriate Client/Sponsor risk categorization and ensure that there is appropriate ongoing monitoring of Client/Sponsor activity and regular updates of CDD.

Based on the three requirements above, the Compliance Officer is responsible for ensuring the appropriate level of CDD evidence is obtained, or its existence confirmed, prior to initiating the Client/ Sponsor relationship. In order to gain the required level of reliance, one of the following may be used:

- reliance on another Department/Sub-Fund where access to CDD information is readily available through shared IT systems; or

If the above do not facilitate collection of the required level of CDD information, the Compliance Manager must ensure additional processes are in place to obtain and retain such information.

4.1.9 Client/Customer Categorization and Approval of PEPs and High Risk

Clients/Customers

Based on the CDD performed, the Client/Sponsor will be categorized in accordance with GIIFs standards as low or high risk. To inform this categorization the following areas should, at a minimum, be considered:

- Client/Sponsor risk:
- Country/geography;
  Entity type (transparency);
- Industry in which entity is engaged or from which an individual sources their funds;
- Political exposure;
- Reputational risk (where applicable).
- Product Risk:
- Complexity;
- Susceptibility to money laundering and terrorist financing (e.g. proliferation of weapons of mass destruction).
- Delivery Channels:
- Non face-to-face;
- Non Residence
- Third party introducers and distributors.

Clients/Sponsors who are categorized as high risk or are PEPs require escalation and approval by either the CEO or his assignee.

4.1.10 Acquisition of Existing Projector Portfolios

When Clients/Sponsors are inherited through the acquisition of another firm and/or portfolio, Departments or appropriate Unit must acquire all underlying CDD records and initiate sample testing to confirm they meet the GIIFs minimum/local standards. Should these standards not be met, the business unit or sub-fund should follow GIIFs standard risk-based methodology for ongoing updates of CDD. The Compliance Manager should select the appropriate sample size in accordance with the size and risk profile of the portfolio being acquired.

4.2 Ongoing Updates of CDD

The information gathered on the Client/Sponsor at take on requires ongoing updates. Department or Business Units/Sub-Funds must apply the CDD standards to existing Clients/Sponsors where required or where the risks warrant.

Department or Business Units/Sub-Funds may determine the nature and extent of the steps required to ensure that they hold appropriate up-to-date information on their Clients/Sponsors based on local requirements and their risk assessment. Ongoing CDD updates must be performed either on a regular basis and / or as a result of a trigger event, such as:

- change of Client/Sponsor details (i.e. Address)
- the report of potential suspicious activity;
- a receipt of a Subpoena;
- any other red flag.

High risk relationships must be reviewed at least annually.

4.3 Ongoing Monitoring of Client/Customer Activity

In support of information gathered at Client/Sponsor take-on and ongoing updates of Client/Sponsor information, monitoring of Client/Customer activity should be undertaken. Different Sponsors/Projects require different types of ongoing monitoring of Client/Sponsor activity. This may be achieved through ongoing interaction with the client/sponsor, such as during visits to the project sites and their offices or the scrutiny of transactions undertaken throughout the course of the relationship through their bankers or the credit reference bureau checks to ensure that their activities are consistent with GIIF's knowledge of the Client/Sponsor and their risk profile. The level and type of ongoing monitoring (standard/enhanced) must be decided by the respective department/Business Unit/Sub-Fund following performance of a risk assessment.

4.3.1 Enhanced Ongoing Monitoring

Business Units/Departments/Sub-Funds must prescribe enhanced ongoing monitoring procedures for Clients/Sponsors that are PEPs and for Clients/Sponsors that present a higher risk of money laundering or terrorist financing. This can take various forms, such as more frequent updates of CDD including public information searches or regular reviews once a year.

4.3.2. Reports of Suspicious Activity

Employees must report any activity where there is knowledge or suspicion, or where there are reasonable grounds for knowing or suspecting that a Client/Sponsor or other person is engaged in money laundering, or terrorist financing, when this information comes to them within the course of business.

Foreign investors with deferred work/resident permits but request for immediate return of their investible funds.

Reports of suspicious activity are highly confidential. In particular, employees must not make any unauthorized disclosure of such reports. Doing so may "tip off" a suspect and compromise an official investigation. In some countries, including Ghana, it is a crime to disclose a Suspicious Activity Report (SAR) other than to the proper authorities.

Employees must ensure that they do not "tip off" suspects that their activity has been identified as suspicious by:

- training Employees on the importance of not "tipping off";
- Maintaining the confidentiality of SARs.

The reporting of suspicious activity is also a part of ongoing monitoring.

All suspicious activities are to be reported to the Financial Intelligence Centre (FIC), Ghana, Established in accordance with section 4 of the Anti-Money Laundering Act, 2008 (Act 749) to receive, analyse and disseminate financial intelligence on Money Laundering and Terrorist Financing in Ghana and abroad. The centre advises on the next level of action to be taken after they investigate the suspicion.

All suspicious activities must first be brought to the attention of the Compliance Manager for further action and reporting to the FIC.

5.0 Restricted Relationships

GIIF will not enter into or maintain relationships with:

- Shell Banks;
- Unlicensed Banks;
- unlicensed and unregistered Money Service Businesses
- any other illegal businesses;
- individuals who are known or suspected to derive their wealth from such businesses;
- Entities or individuals restricted by UN, Europe Union, USA;
- Entities or individuals restricted by France (https://www.tresor.economie.gouv.fr/services-aux-entreprises/sanctions-economiques/dispositif-national-de-gel-des-avoirs
- Bearer share companies, unless the shares are held by a named custodian, with a written undertaking from that custodian that the firm will be notified of any changes to records relating to these shares and the custodian. In exceptional circumstances, the written undertaking may be provided by persons other than the custodian such as law firms or the Ultimate Beneficial Owner. Any variation must be approved with a clear record of reasoning by the Compliance Officer/Manager.

5.1 Record Retention

Business Units/Departments/Sub-Funds must retain records required by this Policy for a period of six years or longer if required by local law and regulations from the date that the Client/Customer relationship ends.

The Compliance Manager should ensure that Records Management does not erase records without determining the date of the end of the Client/Customer relationship within that BU.

6.0 Governance

6.1 Roles and Responsibilities

6.1.1 Senior Management

The CEO or his assistant has overall responsibility within for the establishment and maintenance of effective anti-money laundering systems and controls.

6.1.2 Compliance Manager

The CM shall have a level of authority and independence within the institution and have access to resources and information, sufficient to enable him/her to carry out that responsibility.

CM's responsibilities include but are not limited to:

- overseeing compliance with GIIFs AML Policy as well as relevant legal and regulatory requirements;
- approving the Risk Assessment and Risk-Based Approach;
- producing an annual Compliance report for the business.

6.1.3 Employees

Employees are responsible for ensuring they comply with the terms of this policy and complete all AML training assigned to them in a timely fashion and that they adhere to the necessary requirements of such training, as required by their specific job/role description.

6.2 Policy Review

This Policy is subject to periodic review (at least annually) and revision. The CM, in consultation with CEO, may make changes to the Policy that are consistent with the previously- approved Policy without additional approval. The Compliance Manager should approve any significant changes.

6.3 Policy Oversight and Implementation

Policy Owner: The CM owns this Policy and will review it on a periodic basis or upon changes in relevant legislation.

Approval: CEO

Consulting Committee: Board Risk and Compliance Committee

Implementation: The head of each Business Unit/Sub-Fund has ultimate responsibility for ensuring that their respective business areas establish systems and controls to comply with this Policy.

This includes:

- Taking full account of this Policy when entering into new relationship with all external parties.
- Ensuring that any reliance on third parties or service providers for compliance with this Policy remains reasonable.
- Ensuring all relevant Employees receive appropriate training, with the support of the management and CM in training development and delivery.
- Ensuring conformance of controls in implementing this Policy.
- Ensuring immediate reporting of any breach or suspected breach of this Policy to the CM.

Appendix A

AML Glossary

- **Account**

Any relationship established by GIIF with a Legal Entity or natural person to provide ongoing services, dealings and other financial Transactions including any relationship where an obligation to perform Client/Sponsor identification and/or verification arises under GIIFs Anti-Money Laundering / Terrorist Financing Policy & Procedures. This definition includes Designated Accounts (which are sometimes referred to as sub-accounts).

- **Action Plan**

An Action Plan refers to a pre-defined list of actions and their corresponding due dates that are identified as needing to be undertaken to address:

- An area of Policy for which a Dispensation has been obtained; or
- An area of non-compliance advised by a Breach notification.

- **Address**

For individuals, "address" refers to a residential address. In principle this does not mean a P.O. Box or "care of" (c/o) address. However, specific exceptions to this may arise, for example;

- Postal addresses for military personnel.
- For non-individuals, "address" refers to either a business address, or other address under which the Entity is registered.

- **American Depository Receipts (ADR)**

  An American Depository Receipt (ADR) represents ownership in the shares of a non-US company and trades in US Financial Markets. Each ADR is issued by a US depository bank and can represent a fraction of a share, a single share, or multiple shares of a foreign stock.

- **Bearer Share**

A Bearer Share is a share that is owned by, and gives all rights to, a person whose ownership is not recorded on the company's books.

- **Bifurcated Payments**

A Bifurcated Payment is a Payment transaction consisting of two separate messages being firstly the Payment instruction itself and secondly, an instruction to a third bank to make funds available to the paying bank in cover of the Payment instruction which has usually been sent direct to the paying bank. Also known as a “Cover Payment”.

- **Breach**

A Breach refers to any instance of non-compliance with the Policy that is brought to the attention of the Compliance Manager after the Policy effective date.

- **Business Activity**

A term intended to capture the full range of GIIFs business activities

Business Unit (BU)/Sub-Funds

GIIF terminology referring to a business Unit, a Sub-Fund (this is a creation of the GIIF Act which allows the institution to create sub-funds which may themselves be separate entities operating in a different jurisdiction). A business unit or sub-fund as used may have their own heads who would ultimately be reporting to the CEO.

- **CEO**

Chief Executive Officer of the Ghana Infrastructure Investment Fund

- **Citizenship**

Citizenship is a legal matter, that an individual has been registered with the government of a country as having rights as a full citizen in that country. For most individuals, that is the country where they are born and continue to live, but if a person moves to another country, citizenship may be obtained in the new country, by applying to the government.

For the purposes of this policy citizenship is equivalent to nationality and it is usually determined by the country’s passport or travel document that one bears.

- **Client/Customer**

Client/Sponsor includes any individual or Entity with respect to which GIIF as an entity is obliged to perform Client/Sponsor identification and/or verification under the organization’s Anti-Money Laundering / Terrorist Financing Policy and Procedures. As such, Client/Sponsor includes Related Parties and the designees of Designated Accounts.

It must however be emphasized that, these clients/sponsors will in most instances be promoters of projects submitted to GIIF for financing. The key people who will be driving these projects are referred to as sponsors.

- **Community Institutions**

A public institution, body, office or agency established on the basis of the Treaty on the European Union.

- **Controlled**

An Entity is "Controlled" by the persons or Entities who hold at least 10% of the voting shares in the Entity or who are known to exercise significant influence over the policy, business and strategy of the Entity.

- **Country-Related Entities**

An Entity organized Located, Owned, Controlled, or which conducts Significant Business Activity in a restricted country.

- **Customer Due Diligence (CDD)**

CDD measures are undertaken as part of Anti Money Laundering Policy and procedures. CDD consists of identifying and, where appropriate, verifying the identity of the Client/Sponsor and any relevant related parties such as Owners and controllers and secondly, gathering and recording information to assist in identifying unusual (potentially suspicious) activity.

For the purposes of this Policy the definition of CDD also includes Know Your Client/Customer (KYC) which is part of the due diligence conducted by GIIF prior to the approval of any facility.

- **Designated Account**

An Account that has been opened in one individual's or Entity's name that has been designated to another individual or Entity.

- **Designated Offences**

Designated Offences, according to FATF's Financial Action Task Force on Money Laundering Designated Categories of Offences, as included in The Forty Recommendations, are:

- Participation in an organized criminal group and racketeering;
- Terrorism, including terrorist financing;
- Trafficking in human beings and migrant smuggling;
- Sexual exploitation, including sexual exploitation of children;

- Illicit trafficking in narcotic drugs and psychotropic substances;
- Illicit arms trafficking;
- Illicit trafficking in stolen and other goods;
- Corruption and bribery;
- Fraud;
- Counterfeiting currency;
- Counterfeiting and piracy of products;
- Environmental crime;
- Murder, grievous bodily injury;
- Kidnapping, illegal restraint and hostage-taking;
- Robbery or theft;
- Smuggling;
- Extortion;
- Forgery;
- Piracy; and
- Insider trading and market manipulation.

- **Dispensation**

Temporary exemption from a specific requirement of this Policy.

- **Domestic Payments**

Payments where the originating and beneficiary institutions are both located in the same country and which are not part of a cross-border payment.

- **Electronic Transfer of Funds**

This means all payments made by electronic means, both cross-border (including those made by SWIFT) and non cross-border or domestic payments.

- **Employees**

Employees to whom this Policy applies are:

a. GIIF successful job applicants and employees (both temporary and permanent including those who may be working for a GIIF Sub-Fund/Subsidiary* irrespective of their function, grade or position); and

b. workers (who are not employees) providing services to GIIF under contractual arrangements directly with GIIF including consultants, contractors, non-executive directors, freelancers, and on-call workers.

- **Entity / Entities**

Any organization or legal entity other than an individual person, for example, a company, corporate body, partnership, trust, government agency or charitable organization.

- **Financial Action Task Force**

Thirty-four countries and two regional organizations comprise the membership of the Financial Action Task Force (“FATF”), which has as its mission to establish international standards as well as develop and promote policies, at both national and international levels, in order to combat money laundering and terrorist financing. The principles articulated by FATF have taken the form of two sets of recommendations. The Forty Recommendations from FATF constitute the fundamental framework for combating both money laundering and terrorist financing, with an additional nine Special Recommendations addressing the issue of terrorist financing more specifically. Beyond the FATF membership, more than 130 countries have endorsed the 1996 version of the Forty Recommendations.

- **Government Issued ID**

A government issued identification document is a document which incorporates the Client’s/Sponsors 's full name and photograph and either:

- Residential address; or
- Date of birth.

A government issued document with a photograph includes:

  - Passport
  - Driver's Licence
  - National Identity Card
  - Voter's ID
  - NHIS ID
  - SSNIT ID

- **Integration**

  Integration completes the money laundering process by creating the appearance of legality for underlying criminal proceeds through additional Transactions that provide a plausible explanation for the source of the funds especially where equity is provided towards a particular project by the sponsors/promoters.

- **KYC**

Know Your Client/Customer – see CDD.

- **Layering**

Layering, the second stage of the money laundering process, involves the movement of funds around the financial system, often in a series of Transactions to create a complicated paper trail.

- **Location**

The jurisdiction in which an Entity maintains its primary business premises or the jurisdiction in which it is registered.

- **AMLRO**

Anti Money Laundering Reporting Officer

- **National**

Belonging to a particular nation by birth, citizenship, or naturalization (but excluding those who are Nationals only by reason of having been born to non-Nationals temporarily residing in the country in question, such as the children of non-National aid workers and diplomats).

Non Resident

Non Resident is an individual either a Ghanaian or non Ghanaian living outside Ghana.

- **Owned**

Having a 10% or more legal or beneficial interest in the Entity either directly or indirectly.

- **Owner**

A natural person, listed company or government Entity with a 10% or more legal or beneficial interests either directly or indirectly.

- **Placement**

Placement represents the first and most vulnerable stage of money laundering. The goal is to introduce criminal proceeds into the financial system without drawing the attention of financial institutions or law enforcement.

Common techniques include the structuring of currency deposits in amounts designed to evade reporting requirements or the commingling of deposits flowing from both legal and illegal activities.

- **Politically Exposed Person**

Means, at a minimum:

a. A natural person who has at some stage been entrusted with a prominent public function by:
   i. A state
   ii. A Community institution; or
   iii. An international body; or
b. A close family member of a person referred to in (a); or
c. A close associate of a person referred to in (a); or
d. An entity that is 10% or more owned or controlled by a PEP.

A prominent public officer may include but is not limited to:

- Heads of State, heads of Government and Ministers;
- Senior Judicial Officials;
- Senior Military Officials;
- Senior Judicial Officials;
- Heads and other high-ranking Officers holding senior positions in the armed forces;
- Members of ruling Royal families with governance responsibilities;

- Senior Executives of state-owned enterprises;
- Senior Officials of major political parties.

- **Public Authorities**

Public Authorities in Ghana include but are not limited to government departments, local authorities, schools or public hospitals and the police.

- **Residence**

The current place where an individual ordinarily resides. It will ordinarily be the same as the individual's residential address that the business is required to identify and verify under its AML / KYC / CDD Policy and Procedures.

Resident

An individual ordinarily residing in the named country (*e.g.* for the purposes of employment or study)**.**

- **Securities**

This term relates to equity or debt instruments (or claims related thereto) which are issued by companies listed or regulated on the markets.

- **Supplier**

Individuals or Entities outside of GIIF with which GIIF contracts to procure goods, Technology or services. For the purposes of Screening Entities this extends only to the name and address of the party being contracted with.

- **Suspicious Activity Report (SAR)**

A SAR is a piece of information that alerts law enforcement that certain Client/Sponsor activity is in some way suspicious and might indicate money laundering or terrorist financing.

- **Ultimate Beneficial Owner**

An individual who ultimately owns or controls a Client/Customer and/or the individual on whose behalf a transaction is conducted. This should at least include:

For Corporate Entities Listed on a Regulated Market

any individual who exercises control over the management of the Entity.

For Non-Listed Corporate Entities

- any individual who ultimately owns or controls (whether through direct or indirect ownership or control including through bearer share holdings) more than 10% of the shares or voting rights in that Entity; or
- any individual who otherwise exercises control over the management of the Entity.

For Partnerships*

- any individual who ultimately is entitled to or controls (directly or indirectly) more than a 10% share of the capital or profits of the partnership, or more than 10% of the voting rights in the partnership; or

any individual who otherwise exercises control over the management of the Partnership.

For Trustees

Countries should require trustees of any express trust governed under their law to obtain and hold adequate, accurate, and current beneficial ownership information regarding the trust. This should include information on the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust. Countries should also require trustees of any trust governed under their law to hold basic information on other regulated agents of, and service providers to, the trust, including investment advisors or managers, accountants, and tax advisors”

Entities that Administer and Distribute Funds

- any individual who is the beneficiary of 10% or more of the property of an Entity (where the beneficiaries have been determined);
- any individual who exercises control over 10% or more of the property of an Entity;
- (specifically, for trusts) any individual who has the power to:
  - dispose of, advance, lend, invest, pay or apply trust property;
  - vary the trust;
  - add or remove a person as a beneficiary or from a class of beneficiaries;
  - appoint or remove trustees; or
  - direct, withhold consent to or veto the exercise of a power mentioned above; and

  the class of persons in whose main interest the Entity is set up or operates (where the beneficiaries are yet to be determined). In such a case, the Client/Customer must supply the identity, orally or in writing. When supplied orally, the relevant person must record it in written form.

- **All Other Entities**
  - any individual who is the beneficiary of 10% or more of the property of an Entity (where the beneficiaries have been determined);
  - any individual who exercises control over 10% or more of the property of an Entity;
  - the class of persons in whose main interest the Entity is set up or operates (where the beneficiaries are yet to be determined). In such a case, the Client/Customer must supply the identity, orally or in writing. When supplied orally, the relevant person must record it in written form;
  - in the course of administration of a deceased person, the executor or administrator as indicated by local law; and
  - in any other case, any individual who ultimately owns or controls the Client/Customer, or on whose behalf a transaction is conducted.

  *Excluding limited liability partnerships.

- **Waiver**

  Permanent exemption from this Policy which is subject to regular review, at least annually.

7.0 Policy Control

Authority to approve	Board
Authority to recommend to Board	Risk and Compliance Committee
Policy owner	Chief Risk Officer/Head, Risk & Sustainability
Authority for exemptions	Chief Risk Office (depend on the exemption) Exemption to RAS is Board
Author	Head, Risk and Sustainability
Current version	4.0
Created date	October 2020
Approval date	27th July, 2026
Due for review	20th June, 2028

8.0 Version Control

Version	Revision Date	Author	Description
1.0	10th October, 2020	Risk Manager	AML/CFT Policy
2.0	22nd April, 2022	Risk Manager	AML/CFT Policy
3.0	25th July, 2024	Risk Manager	AML/CFT Policy
4.0	27th July, 2026	Head, Risk & Sustainability	AML/CFT Policy