CGIAR System Organization Anti-Money Laundering and Countering the Financing of Terrorism Policy

Approved by	Executive Director	Policy number	SO CM 02 PL 02
		Risk family	3 – Non-adherence to appropriate values 5 - Poor execution undermines capability
Responsible Official	Director, Legal and Office Services	Version	1.0
		Effective date	21 June 2019

Revision History

Version	Effective date	Approved by	Summary of changes
1.0	21 June 2019	Executive Director	NA

Disclaimer

This is a controlled document. The master document is posted on the CGIAR System intranet. Users may print this document for training and reference purposes but are responsible for regularly checking the CGIAR System intranet for the most current version.

Contents

1. Purpose

This Anti-Money Laundering and Countering the Financing of Terrorism Policy (Policy) sets out the position of the CGIAR System Organization regarding money laundering and terror financing. This Policy is developed with reference to the *International Standard on Combating Money Laundering and the Financing of Terrorism and Proliferation of the Financial Action Task Force*[1]. This Policy is based on the best practices of comparable international organizations.

2. Applicability

This Policy is mandatory and is applicable to the System Organization. Any deviation from this Policy requires a written waiver following the CGIAR System Organization Waiver Procedure and Process (to be developed).

If there is a conflict between this Policy and the requirements of a specific Funder, the Funder's requirements will prevail and the deviations will be documented in writing.

The System Organization may have in place additional Policies, Guidelines, Standard Operating Procedures (SOPs), Business Processes, and Tools to support implementation of this Policy.

Guidelines, SOPs, Business Processes, and Tools may vary with different operating environments if required by local legislation, funder rules and regulations, and other factors, subject to the approval of the Responsible Official.

3. Relevant Definitions

All definitions used within this Policy are governed by the definitions contained in the Accountability Structure Definitions of Standard Terms.

Relevant definitions used within this policy include:
"Know-Your-Counterparty (KYC)" means the process of a verifying the identity of parties and assessing the potential risks for the business relationship;

"ML/FT" means money laundering and financing of terrorism; and

"System Organization resources" means anything of value over which the System Organization has control or responsibility.

[1] http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html

4. Policy

4.1 General

This Policy sets the minimum and mandatory standard to prevent, detect, and investigate money laundering and financing of terrorism, and to control and manage related ML/FT risks.

This Policy is intended to establish effective measures comparable to international best practice to enable the System Organization to:

- Prevent the abuse of System Organization resources for ML/FT including guarding against risks of ML/FT and exercising due diligence; and
- Ensure compliance within the System Organization and with downstream agreements.

The System Organization will take all appropriate measures to prevent corrupt, fraudulent, and otherwise illegal practices, including the prevention of the use of System Organization resources to finance terrorist activity, and to adopt best practice fiduciary principles and standards relating to countering of financing of terrorism and anti-money laundering.

4.2 Risk management

The System Organization will take all reasonable measures to identify, assess, and understand ML/FT risks, document those assessments, and apply resources to ensure the risks are managed and mitigated effectively. For this purpose, the System Organization has adopted a continuous risk-based approach to ensure that measures to prevent, detect, and mitigate money laundering and terrorist financing are commensurate with the risks identified.

The System Organization will ensure that ML/TF risks are effectively managed to mitigate exposure to reputational, financial and legal risks, as well as protect its operations and the integrity of its resources and activities.

At a minimum, the System Organization's ML/FT risk management operations will include:

- A fit-for-purpose AML/CFT Program to effectively control and manage the ML/FT risk;
- An AML/CFT risk assessment designed to identify the risks to which the System Organization is exposed and to assess the effectiveness of the overall AML/CFT Program as required;
- An AML/CFT compliance review to test the effectiveness of AML/CFT controls and to formulate appropriate action plans to address identified control and compliance gaps as required; and
- AML/CFT theme audits as required.

The System Organization will follow the guidance provided by the Financial Action Task Force when considering the types of persons or entities which may present an elevated ML/FT risk. These include but are not limited to:

- Politically Exposed Persons including their immediate family members or close associates, or Politically Exposed Persons-linked entities;
- Financial Institutions providing Correspondent Banking or Money/Value Transfer Services;

- Designated Non-Financial Businesses and Professions;
- Entities issuing Bearer Shares or with nominee shareholders or directors;
- Trusts;
- Entities with unduly complex structure[2] of ownership; and
- Non-profit organizations.

4.3 Know Your Counterparty

The System Organization will undertake appropriate KYC measures when entering into any transaction. KYC measures shall include, at a minimum, identifying and verifying the full identity of the party and the authenticity of that information and screening of all parties against the United Nations Security Council Sanctions List.

Following the risk-based approach, the System Organization may apply more stringent or more specific KYC measures regarding potential or existing parties which are assessed in any one of the categories identified as resulting in an elevated ML/FT risk.

The System Organization will ensure that due diligence is completed before entering into any contractual or financial relationship with a party. Under no circumstances will funds be sent or received before due diligence is completed.

The System Organization will ensure that periodic due diligence reviews of parties are conducted so that emerging risks may be identified early, minimizing any undue consequences and impact to the System Organization. The due diligence review cycle will be determined through the risk-based approach.

4.4 Reporting of suspected ML/FT

System Organization staff and any other individual or entity contracted and/or engaged by or for the System Organization to perform official functions for the System Organization will report any suspicious activity, red flags (indicators of suspicious activity), or ML/TF activity which they identify or suspect, to the Director, Legal and Office Services for investigation. Such reports will be made and investigated in accordance with the System Organizations reporting policies and procedures. Failure to report may result in disciplinary action.

5. Ethical compliance

Any person who has an individual contractual relationship with the System Organization or is engaged to work on behalf of the System Organization and has access to the System Organization intranet and therefore this Policy (such as an employee, consultant, or contractor) is expected to report known or suspected contraventions of this Policy following the procedures set forth in applicable internal policies or available through ethics@cgiar.org.

[2] Unduly complex structure means that a complex structure has been put in place for no apparent purpose, suggesting that it is mainly there to disguise the beneficial owners.

6. Related Documents

6.1 Framework(s)

Risk Management Framework of the CGIAR System (CG CP 02 FM 01)

6.2 Policy(ies)

System Organization Procurement Policy (SO FN 01 PL 01)

6.3 Guideline(s)

To be developed

6.4 SOPs and Business Processes

To be developed

6.5 Tools

To be developed