
# GUIDELINES FOR REPORTING ENTITIES IN CONDUCTING ANTI-MONEY LAUNDERING/COUNTERING TERRORISM OR PROLIFERATION FINANCING (AML/CTPF) COMPLIANCE PROGRAMME INDEPENDENT AUDIT

**MARCH 2021**

## 1.0 INTRODUCTION

In accordance with section 23 (1) of the FIC Act No. 46 of 2010 (as amended), one of theresponsibilities of reporting entities is to develop and implement programmes for the prevention of money laundering, financing of terrorism or proliferation and other financial crimes. . The programmes shall include implementing independent audit arrangements to review and verify compliance with and effectiveness of the measures taken in accordance with the FIC Act.

The purpose of these guidelines is to assist reporting entities in conducting their Anti-Money Laundering/Countering Terrorism or Proliferation Financing (AML/CTPF) Compliance Programme independent audit. The Guidelines will assist reporting entities to understand the AML/CTPF audit requirements and undertake an effective and credible independent audit of their AML/CTPF programme. These guidelines will also be useful to persons who perform independent audits of AML/CTPF programmes of reporting entities.

These guidelines are not legal advice and should not be treated as such. The reporting entity must at all times refer directly to the relevant legislation to ascertain its statutory obligations. The guidelines have been issued in accordance with section 56 and pursuant to section 23 of the FIC Act.

## 2.0 DEFINITION OF KEY TERMS

**Money Laundering**: Under The Prohibition and Prevention of Money Laundering Act No 14 of 2001, as amended by Act No.44 of 2010, a money laundering offence involves various acts committed with the intention to conceal or convert property or the proceeds of property (e.g. money) knowing or believing that these were derived from the commission of a designated offence. In this context, a designated offence means a serious offence as defined in the Forfeiture of Proceeds of Crime Act, 2010. It includes among others those relating to illegal drug trafficking, corruption, bribery, fraud, forgery, murder, robbery, counterfeit money, stock manipulation. A money laundering

offence may also extend to property or proceeds derived from illegal activities that took place outside Zambia.

**Proliferation Financing**: means an act by any person who by any means, directly or indirectly, willfully or negligently provides funds or financial services to be used or knowing that they are to be used in whole or in part for proliferation, the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling, supply, sale or use of nuclear, ballistic, chemical, radiological or biological weapons or any other weapon capable of causing mass destruction and their means of delivery and related materials including both technologies and dual-use goods used for non-legitimate purposes, including technology, goods, software, services or expertise.

**Reporting Entity**: An institution regulated by a Supervisory Authority and required to make a suspicious transaction report to the Centre on suspected Money Laundering, Terrorist Financing and other serious offences under the FIC Act (as amended). Section 2 of the FIC Act has designated various Reporting Entities.

**Risk Based Approach:** Identification of the money laundering risks of customers and transactions which allow us to determine and implement proportionate measures and controls to mitigate these risks.

**Suspicious Transaction Report:** a report submitted on suspected money laundering, terrorist financing or other serious offence, or attempted money laundering, terrorist financing or other serious offence, whether in form of a data message or otherwise.

**Terrorist Financing**: Terrorist financing offences extend to any person who wilfully 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 an individual terrorist. Under the Anti-Terrorism Act No. 21 of 2007 (as amended), it is an offence to knowingly collect or provide property, such as funds, either directly or indirectly, to carry out terrorism or terrorist financing activities.

**Transaction Monitoring**: Scanning and analyzing transactional data for potential money laundering activity. Common approaches to transaction monitoring include the creation of in-house, customizable transaction monitoring rules or engaging a third-party vendor to assist with the development and implementation of automated rules.

## 3.0 WHAT IS AN AML/CFTP INDEPENDENT AUDIT?

Putting your AML/CFTP compliance program into motion is not enough. The program must be monitored and evaluated. Institutions should assess their AML/CFTP programs regularly to ensure their effectiveness and to look for new risk factors. Depending on the jurisdiction, the **"independent audit"** may also be referred to as the **"independent test"** or **"independent review".**

An independent audit is an impartial assessment of the AML/CTPF compliance program of a reporting entity. It checks whether the reporting entity is complying with the AML/CTPF compliance program and that it:

i. properly addresses the Money Laundering/ Terrorism or Proliferation (ML/TPF) risks of the reporting entity
ii. complies with the legal obligations
iii. is working as it should.

The independent audit requirement should be set out in the institutional AML/CTPF policy, which should specifically indicate that an audit shall be independent of the compliance function and may be conducted by either internal or external auditors or persons with AML/CTPF expertise.

## 4.0 WHO SHOULD CONDUCT AN INDEPENDENT AUDIT?

The audit must be independent (i.e. performed by people not involved with the organization's AML/CTPF compliance function) and individuals conducting the audit should report directly to the board of directors or to a designated board committee composed primarily or completely of outside directors. For institutions without board of directors (mostly the Designated Non-Financial Businesses and Professions), the

individuals conducting the audit should report directly to senior management of the institution. Those performing the audit must be sufficiently qualified to ensure that their findings and conclusions are reliable.

The independent reviewer must be someone who:

i. understands the business or organisation
ii. understands ML/TPF risks
iii. was not involved in any part of developing the program, including assessing the ML/TPF risk, developing controls or implementing and/or maintaining the program

The reviewer can be someone in the organisation or someone external to it. An example of an internal reviewer might be an internal auditor. An external reviewer might be a lawyer, an accountant or an AML/CTPF consultant outside the organization who has AML/CTPF knowledge. The reporting entity must make sure there are measures in place to ensure the reviewer's independence.

In assessing how suitable someone is to be an independent reviewer, the reporting entity should consider:

i. whether the independent reviewer belongs to a professional body that requires its members to meet relevant professional standards.
ii. whether the independent reviewer is influenced by the people who were involved in the risk assessment or developing the AML/CTPF compliance programme.
iii. how well the person understands AML/CTPF obligations in relation to the business or organisation.

The reporting entity can engage one reviewer to audit the whole of the AML/CFTP compliance programme or different reviewers for different sections of the programme.

## 5.0 METHODOLOGY AND SCOPE OF THE REVIEW

The methodology that should be applied and the scope of the review should depend on the business or organisation type of the reporting entity. How the independent audit is done and how often it's done depends on the size, nature and complexity of the business or organisation. The ML/TPF risk assessment helps the reporting entity plan the independent reviews. The reporting entity should take into

account the business or organisation's ML/TPF risks and any changes to its business or organisation and/or its risk profile since the last review.

The independent review could examine and/or test some or all of the following:

i. Assess the overall integrity and effectiveness of the AML/CFT compliance program, including policies, procedures and processes.
ii. Assess the adequacy of the AML/CFT risk assessment.
iii. Examine the adequacy of CDD policies, procedures and processes, and whether they comply with regulatory requirements.
iv. Determine personnel adherence to the institution's AML/CFT policies, procedures and processes.
v. Perform appropriate transaction testing, with particular emphasis on high-risk operations (products, services, customers and geographic locations).
vi. Assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule, attendance tracking and escalation procedures for lack of attendance.
vii. Assess compliance with applicable laws and regulations based on the jurisdictions in which the reporting entity does its business.
viii. Examine the integrity and accuracy of management information systems used in the AML/CTPF compliance program. If applicable, this includes assessing the adequacy of the scope of any third-party independent system validations along with the qualifications of parties engaged to perform such reviews.
ix. Review all the aspects of any AML/CTPF compliance functions that have been outsourced from third parties, including the qualifications of the personnel, the contract and the performance and reputation of the company.

x. For reporting entities with transaction monitoring systems or software, the independent review can evaluate the ability of transaction monitoring software application to identify unusual activity by;
    i. reviewing policies, procedures and processes for suspicious activity monitoring;

ii. reviewing the processes for ensuring the completeness, accuracy and timeliness of the data supplied by the source transaction processing systems;
iii. evaluating the methodology for establishing and analyzing expected activity or filtering criteria;
iv. evaluating the appropriateness of the monitoring reports; and comparing the transaction monitoring typologies to the AML/CFT risk assessment for reasonableness.

xi. Review case management and STR systems, including an evaluation of the research and referral of unusual transactions, and a review of policies, procedures and processes for referring unusual or suspicious activity from all business lines to the personnel responsible for investigating unusual activity.
xii. Assess the effectiveness of the institution's policy for reviewing accounts that generate multiple suspicious transaction report filings, including account closure processes.
xiii. Assess the adequacy of record keeping and record retention processes.
xiv. Track previously identified deficiencies and ensures management corrects them promptly.
xv. Decide whether the audit's overall coverage and frequency is appropriate to the risk profile of the organization.
xvi. In coordination with the board or designated board committee, ensure that overall audit coverage and frequency are appropriate to the risk profile of the organization.
xvii. Consider whether the board of directors was responsive to earlier audit findings.
xviii. Determine the adequacy of the following, as they relate to the training program and materials:
a) The importance the board and senior management place on ongoing education, training and compliance.
b) Employee accountability for ensuring AML/CFT compliance, including the employee performance management process.
c) Comprehensiveness of training, related to the risk assessment of each individual business line.
d) Training of personnel from all applicable areas of the institution.
e) Frequency of training including the timeliness of training given to new and transferred employees.

f) Coverage of internal policies, procedures, processes and new rules and regulations.
g) Coverage of different forms of money laundering and terrorist financing as they relate to identifying suspicious activity.
h) Disciplinary actions taken for noncompliance with internal policies and regulatory requirements.

An effective independent reviewer of the AML/CTPF programme will develop and maintain an audit risk assessment to determine audit priorities. They will also develop and maintain detailed audit testing programs for every area.

## 6.0 INDEPENDENT AUDIT REPORT

At the end of the independent audit process, a reporting entity must have a documented report of the review that includes findings and recommendations. The report must be provided to senior management and the board of Directors. The report should be able to show the following:

i. What was tested.
ii. How the tests were done.
iii. The sample sizes used in the tests.

An audit is not complete unless the final audit report is issued by the auditor. The reporting entity may provide a copy of any AML/CFTP independent audit report to the FIC and the supervisor on request or during an inspection. All audit and regulatory recommendations for corrective action must be tracked as well as indicate the target date for completion and the personnel responsible. Regular status reports should be provided to senior management and the board of directors. Supervisory authorities may request them. Failure to properly address audit issues may be a sign of inadequate commitment by senior management and the board of directors with regards to AML/CFTP matters.

## 7.0 HOW OFTEN SHOULD THE INDEPENDENT AUDIT BE CONDUCTED?

A reporting entity must decide how often reviews are done. How a reporting entity decides depends on:

- the size of its business or organisation.

- ❖ the kind of business or organisation it has.
- ❖ how complex its business or organisation is.
- ❖ the level of money laundering/terrorism financing risks.

Reporting entities should have independent reviews done at least once a year. . If the business or organisation has changed significantly, a reporting entity may need to get independent audits done more often. Examples of circumstances that may lead to more frequent reviews include:

i. Structural changes to the business, such as mergers and acquisitions.
ii. Changes to the risks of the business or organisation being used for money laundering or terrorism financing.
iii. Whether the reporting entity has started accepting cash in transactions.
iv. Whether the reporting entity has started outsourcing some of its obligations to another entity.
v. Changes to the number or volume of transactions the reporting entity has.
vi. New customer types.
vii. Whether the reporting entity has had any issues with compliance and any deficiencies previously identified have been remedied.
viii. The status or outcome of any enforcement action taken against competitors.
ix. New products, new designated services or new delivery channels.

There may be other reasons a reporting entity may need to review its AML/CTPF compliance program more frequently. The reporting entity must decide this based on its money laundering/terrorism financing risk profile and its business or organisation.

## 8.0 CONCLUSION

Money laundering is a serious threat to the country's financial system and can have negative consequences at national, sectoral and institutional level. Non-compliance with AML/CTPF regulations can expose the reporting entity to significant regulatory and reputational damage. As such, effective anti-money laundering systems need to be designed to be able to detect and prevent money laundering and the financing of terrorism in financial service providers and Designated Non-Financial Businesses and Professions (DNFBPs). The reporting entity

should ensure that regular independent reviews are conducted on the compliance function in order to ensure that AML/CTPF policy requirements are properly implemented.

**ISSUED BY THE FINANCIAL INTELLIGENCE CENTRE**
**MARCH, 2021**