Guidance Note on Conducting an AML/CFT/PF Audit

(AML/CFT/PF Audit Guidance Note)

NBFIRA

Non-Bank Financial Institutions Regulatory Authority

Contents

1. Purpose 3
2. Scope 3
3. Associated Documents 3
4. Definitions 3
5. Acronyms and Abbreviations 4
6. Responsibility 4
7. Legal Basis for Issuing the Guidance Note 4
7.1 Authority 4
8. Practical Guidelines for NBFIs 5
8.1 AML/CFT/PF Independent Audit 5
8.2 Risk Assessment Review 5
8.3 Compliance Programme Review 5
8.4 Who should conduct an AML/CFT/PF independent audit 5
8.5 Methodology and Scope of the AML/CFT/PF independent audit 6
8.6 Audit Report (Findings and Recommendations) 7
8.7 Management Responsibility 8
8.8 Conclusion 8

1. Purpose

The purpose of the *Guidance Note* is to provide common interpretation for entities to effectively discharge their obligation on subjecting their Anti-Money Laundering, Countering the Financing of Terrorism and Proliferation Financing (AML/CFT/PF) compliance programmes to an independent audit. The guidance is intended to assist entities in understanding AML/CFT/PF audit requirements and conducting effective, credible, and independent audits of their AML/CFT/PF compliance programmes. It also serves as a practical reference for assurance providers engaged to undertake AML/CFT/PF reviews.

2. Scope

This *Guidance Note* applies to all institutions licensed/exempted and supervised by the NBFIRA through various primary and secondary legislation.

3. Associated Documents

The *Guidance Note* should be read in conjunction with the Non-Bank Financial Institutions Regulatory Authority Act; the Financial Intelligence Act; NBFIRA Fit and Proper Rules; NBFIRA AML/CFT/PF Directive 1 and any another relevant regulatory instruments as may be referred to.

4. Definitions

TERM	DEFINITION
Governing body	Refers to the highest-level management structure with accountability for the governance and performance of an entity.
Money Laundering	Has the same meaning assigned to it under the Proceeds and Instruments of Crime Act.
Proliferation Financing	Has the same meaning as assigned to it under the Nuclear Weapons (Prohibition) Act, Biological and Toxin Weapons (Prohibition) Act and the Chemical Weapons (Prohibition) Act (all referred to as the NBC Acts).
Terrorist Financing	Has the same meaning assigned to it under the Counter Terrorism Act.

5. Acronyms and Abbreviations

Abbreviation	Full Form
FI Act	Financial Intelligence Act,2022 (as amended)
AML/CFT/PF	Anti-Money Laundering/Counter the Financing of Terrorism/Proliferation Financing
AMLCO	Anti-Money Laundering & Counter Terrorist Financing Compliance Officer
CDD	Customer Due Diligence
Directive 1	NBFIRA AML/CFT Directive 1
FI Regulations	Financial Intelligence Regulations 2022
ML/TF/PF	Money Laundering/ Terrorist Financing/ Proliferation Financing
NBFIRA	Non-Bank Financial Institutions Regulatory Authority
NBFIs	Non-Bank Financial Institutions

6. Responsibility

Boards of directors or the most senior management, where a board of directors is not present, of NBFIs are accountable and responsible for their entity's compliance with the provisions of the FI Act and all other financial services laws. The responsibility may be delegated to management to ensure compliance during day-to-day business activities as conducted by an NBFI.

7. Legal Basis for Issuing the Guidance Note

7.1 Authority

This *Guidance Note* is issued by NBFIRA, pursuant to its authority provided for under Section 5(2)(d) & (e) of the Non-Bank Financial Institution Regulatory Authority Act, (NBFIRA Act) and Section 49(1)(c) of the Financial Intelligence Act, which empower the Authority to make rules, set standards and provide guidelines for itself and non-bank financial institutions (NBFIs/supervised entities); and give directions to any person to ensure compliance with a relevant law, rule or guideline.

8. Practical Guidelines for NBFIs

8.1 AML/CFT/PF Independent Audit

This is a systematic assessment of the AML/CFT/PF compliance programme (controls, policies, and operations). It evaluates the adequacy of an entity's institutional risk assessment and level of compliance and consistency with its AML/CFT/PF legal obligations and compliance programme. The level of independence may vary depending on whether it is an external or internal review.

The audit is an opportunity for the entity to obtain another view on how well its AML/CFT/PF program is designed and functions.

Section 14(1)(d) of the FI Act obligates specified parties to develop and maintain an independent audit function to examine and evaluate its policies, processes, procedures and controls for compliance with the FI Act and effectiveness thereof. The audit function operates independently from routine operations of the entity, including ongoing AML/CFT/PF activities, and provides unbiased opinion on the entity's AML/CFT/PF efforts.

8.2 Risk Assessment Review

An AML/CFT/PF audit complements the institutional risk assessment process but gives another layer of independent review on whether the institutional risk assessment includes all required areas as per the FI Act and generally accepted risk management principles. An independent auditor is expected to assess the nature and extent of the AML/CFT/PF institutional risk assessment and its application.

8.3 Compliance Programme Review

An AML/CFT/PF audit extends beyond the review of the risk assessment and evaluates the entire control framework (documents and systems) and verifies whether the framework is being complied with on implementation and whether it is compliant with the entity's AML/CFT/PF legal obligations[1]. This should include an assessment of whether the control framework is based on and commensurate with the institutional risk assessment and that it was consistently applied across the entity during the review period.

8.4 Who should conduct an AML/CFT/PF independent audit

Directive 1 requires that the audit be conducted by an "independent person of strong moral standing with technical expertise in Financial Intelligence legislation, financial crimes risks, as well as experience in conducting compliance tests and audits".

[1] AML/CFT legal obligations include all mandatory duties under the FI Act and Directives issued by the NBFIRA.

The auditor need not to be, a Certified Auditor but an independent and sufficiently experienced AML/CFT expert who can give assurance regarding the effectiveness and adequacy of the AML/CFT framework.

Entities may choose to conduct the AML/CFT/PF internal audit either in-house (insource) or through an external service providers (outsource), depending on their size, complexity, and resource capacity. Where the internal audit is **insourced,** the review should be conducted by an independent[2] and suitably qualified employee within an entity, business group, or a related party. Where the internal audit is **outsourced,** review should be conducted by an independent external person or firm with the requisite expertise and competence.

8.5 Methodology and Scope of the AML/CFT/PF independent audit

Directive 1 requires that an internal audit be conducted [every two years at a minimum] to assess and determine the adequacy and effectiveness of the compliance management system (AML/CFT/PF controls). Further, it states that an external audit should be conducted at least once every three years for a more independent and in-depth review. It is important that entities maintain a systematic and risk-based approach to conduct audits which consider the size, nature, and complexity of the business. This would ensure a consistent approach to different audits, helping to meet audit objectives effectively. Furthermore, methodologies with structured procedures that align with best practice may ensure integrity and reliability of the findings.

The Directive prescribes minimum scope for AML/CFT/PF audit, and this must be clearly defined in the audit terms of reference. An entity may extend the scope of its reviews to other areas it considers relevant for effective compliance risk management. Alternatively, the entity may conduct audits in thematic cycles over a defined period, prioritising high-risk areas to ensure that resources are directed where exposure to compliance and financial crime risks are greatest. Other key areas for the audit are the timeframe, business areas, products, and services to be reviewed.

In line with the scope prescribed in *Directive 1*, the review should include but not limit itself to the following:

a) Overall technical adequacy (documentation) and effectiveness (implementation) of the AML/CFT/PF compliance programme, including risk assessments, policies, procedures, processes, systems and controls;
b) The level of governing body and management engagement on corporate and risk governance of the entity;

[2] Independent means not being involved in the entity's AML/CFT/PF risk assessment, or establishing, implementing or maintaining the entity's AML/CFT/PF compliance programme.

c) CDD measures (implementation), including customer identification programme as per their relevant risk profile, and identification of beneficial owners, using relevant information or data from reliable sources;
d) Adequacy of measures taken to reduce the risks associated with establishing and maintaining business relationships with prominent influential persons (PIPs) and their associates;
e) Transaction testing, with emphasis on high-risk elements (products, services, customers and geographic locations);
f) Training; compliance with *Directive 1* and alignment with risk assessment (comprehensiveness, accuracy of materials, training schedule, attendance tracking and escalation procedures for lack of attendance);
g) Compliance with the FI Act or stronger legislation by branches of regulated entities located in foreign jurisdictions;
h) AML/CFT/PF compliance functions that have been outsourced from third parties, including the qualifications of the personnel;
i) Integrity and capacity of information systems used for AML/CFT/PF compliance programme including for record retention;
j) Suspicious transactions/activities reporting process including an evaluation of 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.

In accordance with Section 46(3) of the FI Act, and to safeguard confidentiality while mitigating the risk of unauthorised disclosure, the review should **not** include the following:
a) Review of details of actual Suspicious Activity/Transaction Reports (SAR/STRs) submitted to FIA
b) Review of details of actual Suspicious Activity/Transaction Reports (SAR/STRs) pending submission to FIA.
c) A prudential assessment (non-AML/CFT/PF based) review.

8.6 Audit Report (Findings and Recommendations)

At the end of the audit process, the auditor must submit [to the governing body] a documented report of the review reflecting factual findings and recommendations. The findings should provide details on the extent of compliance with the institutional risk assessment and the entire compliance programme with AML/CFT/PF obligations, and whether such programme is being implemented and practiced as required and intended. The report should include other standard details such as methodologies used, audit period, and title of the report detailing the type of audit.

A supervised entity is expected to submit the audit report upon request by the Authority. Where, upon review, the Authority deems the audit deficient, it may reject the audit report and direct the entity to conduct a further audit.

8.7 Management Responsibility

The governing body of an entity is accountable and responsible for an entity's compliance with provisions of the FI Act and other financial services laws. The responsibility may be partly delegated to executive management to ensure compliance during day-to-day business activities as conducted by an entity. However, the appointment of an auditor and setting of terms of reference of the auditor should remain exclusively within the mandate of the governing body to preserve independence and proper oversight.

The governing body, together with senior management, should study the report, its findings and recommendations, and develop an action plan to remediate identified gaps. The timeframe for closing gaps should be risk-based and reasonable to ensure effective closure of audit findings. Furthermore, in determining action timelines, it is crucial to consider gravity of the findings and possible compliance and financial crime risks. The governing body should ensure monitoring of the action plan and ensure it satisfies itself that corrective actions have been fully implemented.

8.8 Conclusion

Independent audits are useful in testing the effectiveness of an AML/CFT/PF framework. When established and conducted in a correct manner, they tend to complement risk assessment and self-reviews by providing critical reviews from an unbiased position thereby preempting regulatory sanctions. Therefore, entities are encouraged to consider audits as part of a starting point and means to full compliance, rather than just a compliance issue.