



هيئة الأوراق المالية والسلع  
SECURITIES & COMMODITIES AUTHORITY



**Minimum Standards for  
Semi-Annual  
Anti-Money Laundering  
and  
Counter-Terrorism Financing  
Report  
2023**



## **Introduction:**

This document serves as an indispensable guide for the creation of Compliance Officer (CO)/ Money Laundering Reporting Officer (MLRO) report focused on compliance with Anti-Money Laundering (AML) and Counter-Terrorism Financing (CFT) regulations in the United Arab Emirates (UAE). It specifically caters to securities firms, including Virtual Asset Service Providers (VASPs) licensed by the Securities and Commodities Authority (SCA) in the UAE.

In the UAE, the CO/MLRO report is a crucial communication tool for both senior management and regulatory authorities, demonstrating the institution's commitment to maintaining high standards of AML/CFT and TFS compliance. The minimum standards contained within this document are designed to provide MLROs with the necessary tools to prepare detailed, coherent, and effective reports.

While this document provides a comprehensive outline for creating an MLRO report, it is essential to adapt it to reflect the unique characteristics, operations, and risk profiles of individual institutions. This includes consideration of the institution's size, customer base, products and services, geographical reach, and identified risks.

## **Objective:**

The CO/MLRO report is an essential tool in demonstrating a firm's AML/CFT and TFS regulations set out by the UAE legislations. The report provides a comprehensive review of the firm's AML/CFT practices, identifying any challenges, breaches, or areas for improvement that transpired during the reporting period. It covers an array of elements, including internal controls, risk assessments, due diligence measures, reporting obligations, and training initiatives.

The MLRO report also serves as a critical instrument for senior management and the Board of Directors, allowing them to understand the current state of the firm's AML/CFT compliance, and assess the effectiveness of existing policies and procedures. In the context of the UAE, the report showcases the firm's compliance with local legislation,

including Federal Decree-Law No. 20 of 2018 and Cabinet Decision No. 10 of 2019 and its amendments.

## **Legal Background and Legislation in the UAE**

The legal framework for AML/CFT compliance in the United Arab Emirates (UAE) is primarily defined by Federal Decree-Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations. Further to this, Cabinet Decision No. 10 of 2019 provides implementing regulations for the Decree Law. This legislation mandates that Financial Institutions appoint a compliance officer (MLRO) with appropriate competencies and experience.

The compliance officer's (MLRO's) key responsibilities include reviewing internal rules and procedures relating to combating financial crime, assessing their consistency with the Decree Law and Cabinet Decision, and evaluating the extent to which the institution upholds these rules and procedures. They are also tasked with proposing necessary updates to these rules and procedures, preparing, and submitting semi-annual reports on these points to senior management. A copy of these reports, along with senior management's remarks and decisions, must be submitted to the relevant Supervisory Authority.

## **Roles and Responsibilities in Bi-Annual Compliance Reporting**

This section outlines the roles and responsibilities involved in the bi-annual compliance reporting process for financial institutions operating under UAE jurisdiction and licensed by SCA. These standards delineate the duties of various stakeholders, including CO/MLRO, senior management, and the Board of Directors.

Financial institutions operating in the UAE and licensed by SCA have a set of obligations that need to be met regarding bi-annual compliance reporting. These reports provide an overview of the organization's AML/CFT activities over the previous six months and are pivotal in maintaining transparency and adherence to regulations.

- A thorough process must be in place for creating and submitting these bi-annual compliance reports to the SCA. These reports must give an overview of the

institution's compliance with AML/CFT regulations, with a particular focus on any challenges or issues that have arisen during the reporting period.

- it's imperative that these reports are accurate and comprehensive, covering the preceding six months' worth of compliance activities and issues. Prior to submission, these reports must be meticulously reviewed and approved by both senior management and the Board of Directors. This ensures that the data provided to the SCA accurately reflects the institution's compliance status and any related issues.
- A process should be established to address any issues or concerns identified by the SCA during their review of the bi-annual compliance report. This responsiveness is critical in maintaining open communication and swiftly resolving any potential compliance issues.
- Moreover, financial institutions need to maintain records of the bi-annual compliance report and any related communication with the SCA. This record-keeping facilitates an ongoing review of compliance efforts and provides a historical reference for future compliance activities.
- The CO/MLRO is tasked with preparing the Bi-Annual Compliance Reports, which assess the effectiveness of the institution's AML/CFT policies, procedures, systems, and controls. These reports, covering the six-month periods ending on 30<sup>th</sup> June and 31<sup>st</sup> December of each financial year, act as an integral tool in preventing money laundering and terrorist financing.
- The recipients of these reports are the top management and the Board of Directors. In instances where there is no Board of Directors, the Owner or Partners assume this responsibility, ensuring that these critical reports are reviewed at the highest level within the institution.
- The financial institution must send a copy of the Bi-Annual CO/MLRO Report to SCA along with comments from the Board of Directors (or from the Owner/Partners where there is no Board of Directors) within two (2) months from the end of each reporting period.

### **Structure for MLRO Report**

The below structure of the CO/ MLRO Report is designed to provide a holistic review of the organization's AML/CFT and sanction compliance program. It begins with an executive summary and introduction, followed by a detailed assessment of the compliance program, a gap analysis, and a proposed action plan for the coming period. The report concludes with key findings, recommendations, and a statement of approval from the Board of Directors (or the Owner/Partners where there is no Board of Directors), before being submitted to the SCA.

## I. Executive Summary

The Executive Summary is the starting section of the MLRO report. It provides a quick, easy-to-understand overview of the main points of the report. This part of the report is very important because it offers a brief snapshot of the most important findings, any risks that were discovered, and what actions need to be taken.

- **Key Findings:** This part summarizes the main discoveries of the report. This might include important information about how well the organization is doing in terms of AML/CFT and sanction compliance and any compliance issues that were found.
- **Identified Risks:** This section highlights any risks that were found. This could be new risks, areas where the organization's controls might not be strong enough, or parts of the organization that have a high risk of money laundering or terrorism financing.
- **Recommended Action Points:** This part outlines what actions the organization should take based on the findings and risks that were identified. This could include changes to how things are done, improvements to systems or controls, or areas where more training is needed.

## II. Assessment of the AML/CFT and Sanction Compliance Program

The section provides a comprehensive evaluation of the organization's current AML/CFT and sanction compliance program. This part of the report is intended to gauge how effective the program is at preventing money laundering and

terrorist financing activities. It does so by examining various below elements of the program in detail:

- **Governance Controls:** This subsection should discuss the governance controls in place for the AML/CFT and sanction compliance program. This includes the oversight and management of the program, including how decisions are made, how the program is structured, and who is responsible for its management. It should also evaluate how effective these governance controls are at ensuring the program's effectiveness and compliance with regulatory requirements.
- **Enterprise-Wide Risk Assessment (EWRA):** This subsection should evaluate the organization's business-wide risk assessment process. This process should identify the money laundering and terrorist financing risks the organization faces, considering factors like its size, nature, and complexity, as well as the countries and sectors it operates in. The assessment should consider whether the BWRA is comprehensive, up-to-date, and effectively used to inform the organization's AML/CFT and sanction compliance program
- **Policies and Procedures:** This subsection discusses the FI's existing AML/CFT and sanction compliance policies and procedures. It evaluates their effectiveness and identifies any areas where improvements can be made. It might cover how well these policies and procedures are understood and followed across the organization and if they are up-to-date with the latest regulations and best practices.
- **Customer Risk Rating:** This part of the assessment looks at how the organization rates the risk associated with each customer. It evaluates whether the risk rating process is effective and consistent, and whether it accurately reflects the level of risk associated with each customer.
- **Simplified Due Diligence (SDD), Customer Due Diligence (CDD), Enhanced Due Diligence (EDD):** This part of the assessment examines the FI's due diligence processes. It evaluates how effectively these processes identify and assess the risk associated with each customer. This might involve discussing how the organization determines which level of due

diligence is appropriate for each customer and whether there are any areas for improvement.

- Ongoing Monitoring: This subsection reviews the processes in place for monitoring customers' activities on an ongoing basis. It assesses how effective these measures are at identifying suspicious activity and whether there are any gaps in the monitoring processes that could be addressed.
- Screening: This subsection evaluates the FI's screening processes and tools. It might discuss how effectively these tools identify customers who pose a risk and whether there are any gaps or areas for improvement.
- PEP Transition Monitoring: This subsection should assess how the FI identifies and monitors Politically Exposed Persons (PEPs). This should include an evaluation of the processes and tools used to identify PEPs during the customer due diligence process, and how the organization monitors PEPs for potential money laundering or terrorist financing risks.
- Training and Awareness: This subsection should assess the quality and effectiveness of AML/CFT and sanctions training provided to employees. This could involve discussing how frequently training is provided, whether it is tailored to the roles and responsibilities of different employees, and how well employees understand their AML/CFT and sanctions obligations.
- Record Keeping: This subsection should evaluate the FI's record-keeping practices, assessing whether records are maintained in a manner that complies with relevant legal and regulatory requirements.

### III. Action Plan

The "Action Plan" section is designed to address both identified deficiencies and areas where enhancements to the AML/CFT and sanction compliance program are needed. It aims to provide a strategic and actionable roadmap to remediate any shortcomings and to ensure continuous improvement in the organization's compliance function.

Key elements of the Action Plan might include:

- Proposed Actions: This is a list of specific steps that the organization plans to take to improve its AML/CFT and TFS compliance functions. Each action should be clearly defined, with a clear objective and a timeline for

completion. Actions might include things like updating policies and procedures, implementing new technology solutions, or providing additional training to staff.

- **Responsibilities:** For each proposed action, the report should specify who within the organization will be responsible for implementing it. This helps to ensure accountability and facilitates follow-up.
- **Metrics for Success:** The action plan should also include clear metrics for evaluating the success of each proposed action. This could involve both quantitative measures (such as the number of staff trained) and qualitative measures (such as improvements in staff understanding of AML/CFT and TFS requirements).
- **Status Update on Previous Action Plan:** This part of the action plan provides an update on the actions proposed in the previous MLRO report. It should detail the progress made on each action, including any actions that have been completed, any that are still in progress, and any that were not started or were delayed. If any actions were not completed as planned, the report should explain why and what steps will be taken to address this.
- **Risks and Challenges:** The action plan should also identify any potential risks or challenges that could impact the implementation of the proposed actions. This could include things like resource constraints, technological challenges, or changes in the regulatory environment.

#### **IV. Conclusion and Recommendations**

- The "Conclusion and Recommendations" section wraps up the report by summarizing the key findings from the assessment and the gap analysis. This provides an overall impression of the current state of the FI's AML/CFT and sanction compliance program, highlighting both strengths and areas for improvement.
- In this section, any limitations in the existing systems and material resource gaps that could affect the compliance program's effectiveness should be noted. These could include technological constraints, insufficient staffing, or lack of specific expertise.

- Based on the identified risks and issues, recommendations are then made to improve the compliance program. These could be specific actions, such as revising certain policies or implementing new monitoring tools, or more strategic suggestions, such as enhancing employee training or engaging external expertise. These recommendations are typically framed in a way that provides a clear path forward for the FI to further strengthen its compliance program.

## V. Approval and Submission

- This section is the final part of the report. It indicates that the Bi-Annual CO/MLRO report has been reviewed and approved by the FI's highest level of authority - the Board of Directors, or the Owner/Partners in cases where there is no Board of Directors. This approval signifies that the senior management has read, understood, and endorsed the findings and recommendations of the report.
- This section also notes that a copy of the report will be submitted to SCA. This will be done along with any comments or feedback from the Board of Directors (or from the Owner/Partners where there is no Board of Directors) within a specified period (two months) from the end of the reporting period.

## VI. Appendices

This section should include any relevant supporting information or documents, such as detailed statistics, audit reports or training materials. Below are examples of compliance indicators that can be included:

1. Number of high-risk customers identified
2. Number of high-risk transactions identified
3. Number of customer complaints related to AML/CFT
4. Number of internal and external audits related to AML/CFT
5. Number of identified instances of non-compliance with AML/CFT regulations
6. Number of Suspicious Activity Reports (SARs) filed
7. Number of employees trained in AML/CFT
8. Number of updates or changes made to AML/CFT policies and procedures

9. Number of interactions with regulators and law enforcement related to AML/CFT.
10. Number of internal risk assessments conducted.
11. Number of times AML/CFT software or technology systems were updated or audited.
12. Number of identified unusual or complex transactions that warrant further investigation.
13. Number of regulatory breaches identified and resolved.
14. Number of AML/CFT-related investigations conducted by internal or external bodies.
15. Number of identified cases of Politically Exposed Persons (PEPs).