

By email

28th November 2024

To Senior Executive Officer (SEO) of FSRA Authorised Firms
Cc: Compliance Officer (CO) and Money Laundering Reporting Officer (MLRO)

Dear SEO,

Thematic Review on Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Overall Observations

In line with our regulatory objectives, and our 2024 supervisory priorities, FSRA Supervision undertook a detailed Thematic Review (Review), across all Authorised Persons (APs), to assess the effective implementation of AML/CFT frameworks (including ADGM Rules and Regulations, along with the relevant UAE Federal Legislation).

The purpose of this letter is to share the key findings and general observations from the Review to promote best practice and high standards of regulatory compliance by APs, as part of FSRA's ongoing efforts to strengthen Anti-Money Laundering (AML), Counter Financing of Terrorism (CFT) and Targeted Financial Sanctions (TFS) measures within the ADGM.

Background and Scope

The Thematic review assessment covers a wide range of APs across various activity types and business models, offering a comprehensive overview of industry practices and potential vulnerabilities. The scope set out was to cover the following key areas:

- a) **Risk-Based Approach:** Evaluating how APs design and implement a robust risk-based approach to managing AML/CFT and TFS risks.
- b) **Customer Due Diligence (CDD):** Assessing the effectiveness of onboarding processes to ensure adequate understanding of clients and associated risks.
- c) **Targeted Financial Sanctions (TFS):** Reviewing the systems and controls in place to ensure compliance with UAE sanctions obligations and to identify and manage potential exposure to sanctioned individuals and entities.
- d) **Suspicious Activity and Transaction Reporting:** Evaluating firms' processes for detecting, investigating, and reporting suspicious activities or transactions in a timely manner.

Approach adopted

This Review consisted of two phases: a broad quantitative assessment conducted on all the APs followed by a focused qualitative on-site assessment of selected firms, based on a risk-based assessment of the AML/CTF, and TFS practices of APs.

1- Quantitative Assessment:

Industry-Wide Survey: On 10 June 2024 a communication was sent to all APs with active financial services permissions that included a survey in order to collect data on:

- Client Base: Number of clients, demographics, and risk profiles.
- Business Activities: Transaction volumes, geographic operations, and services provided.
- Risk Exposure: Potential risks related to client activities and jurisdictions.

Data Analysis and Sampling: The survey data responses were analysed to identify APs with higher exposure to AML/CFT and TFS risks. Based on this analysis, a sample of firms was selected for a detailed on-site review.

2- Qualitative Assessment:

On-Site Reviews: These on-site reviews focused on the key areas outlined in the Review's scope, including:

- AML/CTF/TF Framework: Evaluating the effectiveness of the firm's policies and procedures in the identified areas.
- Operational Execution: Reviewing how well the framework was implemented.
- Systems and Controls: Assessing the relevant systems and controls in place to identify, assess, and manage the risks.

Key Findings

Prevention of Financial Crime is fundamental to the FSRA's mandate and aligns with the UAE's national agenda. This focus is important for safeguarding the reputation of the ADGM and will remain a key priority in our reviews and engagement activities.

While we have noted overall improvements in the development of policies, procedures, systems and controls adopted by APs, the thematic review has identified some repeated but also new findings compared to last year's review.

New findings that require attention regarding particularly the record-keeping practices for customer due diligence (CDD). to ensure that CDD documentation is maintained in full alignment with regulatory requirements.

In addition to these new findings, we also observed recurring issues, particularly related to the documentation adequacy in firms' business risk assessments and customer risk assessment methodologies. For business risk assessments, clear and comprehensive documentation should reflect a firm's approach to managing identified risks across its operations, taking into account the scale, nature, and complexity of its business. Similarly, customer risk assessments should be designed, documented and effective to ensure they fully reflect the money laundering risks associated with the customer in a transparent, clear and a structured approach.

Next Steps

The FSRA expects firms to assess their current frameworks against the Review findings and implement enhancements to meet the respective compliance expectations. Consistent and effective financial crime controls are essential for sustaining a secure business environment, and senior management is expected to play an active role in driving these improvements across all levels of the firm. Where specific concerns in relation to specific APs have been identified, these will be addressed directly with the firm concerned

For a detailed overview of the FSRA's expectations based on the findings from this review, firms should refer to the Appendix.

In case of any queries, please do not hesitate to contact the FSRA Supervision team.

Sincerely,



Mary Anne Scicluna
Senior Executive Director - Supervision
Financial Services Regulatory Authority

Appendix 1

Observations and Themes	
Risk Based Approach AML 6 - Business Risk Assessment and AML 7 - Customer Risk Assessment	<p>A Risk-Based Approach (RBA) is a cornerstone of effective AML/CTF frameworks. It enables firms to allocate resources in proportion to the level of risk identified across different activities.</p> <p>Identification of Risks is one of the foundational aspects of a RBA and Business and Customer Risk Assessments (BRA and CRA) are key factors in this regard.</p> <p>The following sections outline key areas for improvement in the BRA and CRA processes, focusing on enhancing documentation, control implementation, and overall effectiveness to meet industry best practices and regulatory expectations</p> <p>Business Risk Assessment (BRA):</p> <ul style="list-style-type: none"> • BRA Implementation and Documentation: <p>All firms should have a well-documented and fully implemented BRA methodology, supported by relevant quantitative data relevant to the firm's nature, scale, and complexity. While some firms have structured BRA approaches, they often lack sufficient evidence of implementation, such as effectiveness testing results for each control. Furthermore, firms must ensure their BRA comprehensively addresses all relevant risks, including AML, terrorist financing, and proliferation financing, as per AML Rulebook 6.1.1</p> <ul style="list-style-type: none"> • Risk Assessments for New Products and Services <p>Consistent with AML Rulebook 6.1.3, all firms must conduct comprehensive risk assessments before introducing new products, services, or technologies to capture any potential AML/CTF risks. Not conducting a BRA before launching new products can lead to oversight of inherent AML risks. Firms should ensure that new business activities, technologies, or client segments are thoroughly assessed with appropriate controls implemented to mitigate any new risks identified.</p> <p>Customer Risk Assessment (CRA):</p> <ul style="list-style-type: none"> • Clear Documentation and Methodology in Customer Risk Assessments <p>All firms are expected to establish a CRA methodology that is thoroughly documented and transparent, outlining each step of the risk assessment process in detail. This documentation should clearly specify the criteria and processes used to</p>

	<p>assess customer risks, providing a complete view of the approach from start to finish. Detailed documentation enables firms to track and justify each risk assessment decision, ensuring consistency and reinforcing the CRA's reliability. A well-documented CRA framework also strengthens the firm's ability to effectively manage and mitigate customer-specific risks</p> <ul style="list-style-type: none"> Balanced and Comprehensive Design of Customer Risk Assessments The CRA design should offer a balanced and comprehensive view of customer risks, capturing the entire range of money laundering risks without being structured to produce predominantly low-risk ratings. The CRA framework should incorporate a quantifiable risk rating system that objectively and consistently evaluates a variety of risk factors. In some instances, CRA designs have been limited in scope or have relied on subjective criteria, which can lead to inconsistent or unsupported risk ratings. By implementing a balanced CRA structure, firms can ensure a more accurate assessment of each client's risk profile in order to reflect the wholistic money laundering risks that maybe associated with the customer, enabling them to allocate resources proportionately and address potential vulnerabilities effectively. Documented CRA Overrides and Methodology All firms are required to maintain a transparent and well-documented CRA framework that supports objectivity in customer risk assessments. Instances identified where CRA tool-generated ratings are overridden without documented justification, undermining the CRA process. Any overrides of CRA tool-generated ratings should be thoroughly documented and governed by a structured internal approval process to ensure consistency and accountability. This approach provides clear justification for any adjustments, reinforcing the integrity of the CRA process and preventing arbitrary changes that could compromise the accuracy of risk assessments.
AML 8 - Customer Due Diligence	<p>Customer Due Diligence (CDD) is a vital component of any effective AML/CTF program. Through CDD processes, firms can assess and understand the potential risks associated with their clients, helping to prevent financial crime and ensure regulatory compliance. The following sections highlight key focus areas for enhancing CDD processes. Emphasizing these elements can help firms strengthen their CDD practices, mitigate risks, and maintain robust compliance with AML/CTF expectations.</p> <ul style="list-style-type: none"> Improving Identification and Verification of Ultimate Beneficial Owners (UBOs)

	<p>All firms are required to implement strong controls to ensure that UBOs are thoroughly identified and verified prior to onboarding. This step enhances regulatory compliance and reduces potential risks associated with unidentified beneficial owners.</p> <ul style="list-style-type: none"> Enhanced Due Diligence (EDD) Procedures When conducting EDD, firms are required to implement additional measures to mitigate client-related risks, such as Source of Wealth (SoW) and Source of Funds (SoF) verification for high-risk clients and UBOs, along with obtaining senior management approval in line with AML Rule 8.4.1. Consistent EDD implementation strengthens risk controls and supports a proactive approach to managing higher-risk client relationships. Expanding Documentation Standards for Address Verification Documentation for address verification should be standardised to ensure accuracy and full compliance with regulatory requirements related to address verification. Clear guidelines on acceptable address proof ensures thorough record-keeping and support the quality of due diligence. Enhancing Documentation Practices in Onboarding Records All firms are required to maintain complete and accurate onboarding and ongoing records of their client, even when transitioning between service providers. Firms are encouraged to maintain these records inhouse where possible and ensure they have put proper business continuity measures in place. Streamlined documentation practices enhance data integrity and support strong compliance foundations. Enhancing Identity Verification in Digital Onboarding For firms that have adopted digital onboarding for clients, it is important to integrate advanced verification techniques, such as facial recognition or equivalent biometric authentication methods, into their onboarding processes. Such enhancements strengthen identity assurance and align with evolving digital verification international standards and reduce the risk of impersonation or fraud. Documenting the approach for Politically Exposed Persons (PEPs) During our thematic review, we observed some confusion regarding PEP risk classification and due diligence. We would like to reiterate the importance of adhering to the FSRA's AML Rulebook and Cabinet Decision No. 10 of 2019, which provide clear guidance on managing PEP risks.
--	--

	<p>While the FSRAAML Rulebook does not mandate classifying all PEPs as high-risk, it does emphasize the heightened money laundering risk associated with PEPs and more specifically the Foreign PEPs. Regardless of the risk classification, firms are required to conduct enhanced due diligence (EDD) when a PEP is identified, whether at onboarding or during periodic reviews.</p> <p>Furthermore, we would like to highlight that the presence of a PEP on the Board of a legal entity does not automatically classify that entity as a PEP or high-risk client, nor does it imply that EDD must be applied by default. Instead, firms should factor this information into their customer risk assessment process and based on this, firms should then determine the appropriate level of due diligence.</p>
AML 11 - Targeted Financial Sanctions	<p>The key themes for Strengthening Sanctions Screening and Documentation Practices:</p> <ul style="list-style-type: none"> Maintaining Evidence of Screening Against UAE and International Sanctions Lists All firms are required to retain documented evidence of the screened clients against relevant sanctions lists, including the UAE Executive Office of the Committee for Goods and Materials Subject to Import and Export Control (EO) lists and UN sanctions. Ensuring complete coverage of entries from these lists enhances regulatory compliance and supports transparency. Conducting Comprehensive Initial and Ongoing Sanctions Screening All firms must perform both initial and ongoing sanctions screening for all clients. This includes screening against UN and UAE IEC sanctions lists at onboarding and periodically thereafter. Clear documentation of all screening activities is important for effective risk management and regulatory adherence. Implementing Transaction Screening as Part of Sanctions Controls All firms are required to conduct transaction screening of all parties involved in transaction, alongside customer screening to capture any sanctions-related risks during transactions. Relying on other financial institutions for this function may create gaps in sanctions compliance. Therefore, the firms are expected to enhance the controls and fill in the gaps. Documenting the Review Process for Sanctions Screening System Adequacy Regular assessments of sanctions screening systems should be conducted and documented to ensure effectiveness and that the screening lists are aligned with the FSRA rules and the federal regulations. These periodic reviews should be recorded

	<p>and maintained to confirm that the systems are operating as intended and to identify any areas for potential improvement.</p> <ul style="list-style-type: none"> • Recording Rationale for Determining False Positives Documenting the rationale when determining that a sanctions hit is a false positive is essential. Proper recording of these decisions improves transparency and supports effective review of the decision-making process, contributing to an accurate and reliable sanctions compliance framework.
AML 14 - Suspicious activity reporting	<p>To enhance the effectiveness of suspicious activity reporting and monitoring systems and controls, firms are encouraged to focus on the following key areas:</p> <ul style="list-style-type: none"> • Ensuring Timely Registration on Reporting Platforms All firms are required to ensure that CO/MLRO promptly register on necessary regulatory reporting platforms, such as goAML, upon appointment or any changes. Timely registration facilitates efficient reporting and enables the firm to meet the regulatory and Federal obligations effectively. • Enhancing Documentation for Third-Party Transactions All firms are expected to maintain comprehensive documentation and due diligence for third-party transactions to justify their purpose and nature. Ensuring that adequate records are available for transactions involving unfamiliar parties. strengthens AML controls and supports risk assessment, particularly for non-typical transactions that may indicate potential AML risks. • Developing a Targeted Suspicious Transaction Monitoring Approach for Fund Activities Fund managers are expected to establish specific procedures for monitoring suspicious transactions related to fund activities, including subscriptions and redemptions. Implementing this approach to detect unusual fund transactions enhances the firm's ability to identify and address potential AML risks associated with fund management activities.