10 April 2026

Notice No: FSRA/FCCP/62/2026

To: Senior Executive Officers (SEO), Money Laundering Reporting Officers (MLRO) and Principal Representatives (PR) of Approved Persons

Dear SEO/MLRO/RP,

RE: Guidance on Business Risk Assessment

The Financial & Cyber Crime Prevention (FCCP)-FSRA issues this guidance to clarify regulatory expectations and to assist firms in preparing/conducting a Business Risk Assessment (BRA). A robust documented of BRA is both a legal and supervisory requirement and forms the foundation of an effective, risk-based anti-money laundering, counter-terrorist financing and counter-proliferation financing (AML/TFS/PF) programme.

Scope and objectives

The guidance sets out key factors and measures the Relevant Persons (RP) should consider when conducting a BRA. It is not exhaustive and does not limit the other reasonable approaches firm may adopt, steps provided to comply with applicable laws and regulations. In the absence of a prescribed methodology, RPs should implement a documented approach that is proportionate to the nature, scale and complexity of their business, incorporating relevant risk factors and mitigating measures.

Legal Basis

The requirement to perform and document a BRA arises from:

1. Rule (6) of the Anti-Money Laundering and Sanctions Rulebook (AML).
2. Decree Federal Law No. 10 of 2025 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations; and
3. Cabinet Decision No. 134 of 2025 Concerning the Implementing Regulation of Decree Federal Law No. 10 of 2025 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations.
4. Cabinet Decision No. 74 of 2020 Concerning the UAE list of terrorists and implementation of UN Security Council decisions relating to preventing and countering financing terrorism and leveraging non-proliferation of weapons of mass destruction, and the relevant resolutions.

Key requirements

1. Governance and Oversight

Relevant Persons are expected to establish a clear governance framework for the BRA. Responsibility for conducting and maintaining the BRA must be clearly assigned to the MLRO, with the board or senior management overseeing and formally approving the BRA. The outcomes must be embedded/integrated into firms' risk management and compliance framework, informing decision-making and resource allocation.

2. Identifying Inherent Risks

RPs must identify the inherent ML/TF/PF risks to which their business is exposed. These risks exist prior to the implementation of any controls. They should differentiate between ML, TF, and PF risks and assess them across the following core categories:

- **Customer Risk**: RPs must evaluate the nature and profile of the customer base, considering factors such as customer type (individuals, legal persons, VASPs), geographical origin, industry, business practices, ownership structure, and whether they are classified as high-risk, such as politically exposed persons (PEPs) or non-residents.
- **Geographic Risk**: Geographic exposure must be assessed based on the countries where clients or counterparties reside, operate or conduct transactions. Jurisdictions which are not compliant with international AML/TFS standards and identified as high-risk by international bodies such as FATF, must be carefully considered in the BRA.
- **Product and Service Risk**: Consideration must be given to the types of products and services offered by the customer. Some products may carry higher risks of misuse for ML/TF/PF, particularly where they involve anonymity, complex structures, rapid movement of funds or Dual-Use Good.
- **Delivery Channel Risk**: The means through which products and services are delivered should be assessed. Channels involving non-face-to-face onboarding, digital platforms, intermediaries, or agents may present increased risks and should be evaluated accordingly.
- **Transactional Risk**: RPs must assess transaction volumes, patterns, and behaviors including the nature, size, frequency and complexity of the transactions. Unusual or high-volume transactions, particularly those inconsistent with the customer profile or transactions involving high-risk countries may indicate elevated risk.
- **New Developments and Technologies:** RPs must evaluate the specific new developments and technologies being introduced, such as cryptocurrency, blockchain, artificial intelligence, or machine learning, and their potential to facilitate ML/TF/PF activities. This includes evaluating features like anonymity, cross-border transactions, and the ease of encryption, all of which could pose risks in facilitating illicit activities if not properly managed.
- **Emerging ML/TF/PF Risks:** It is essential that systems and controls are in place to identify and assess emerging ML, TF, and PF risks, or existing risks that have increased over time. Where necessary, these risks should be incorporated into the BRA in a timely manner to ensure that appropriate measures are taken to mitigate them and reduce exposure.
- **Any other relevant factors specific to the business:** In addition to the above, RPs should consider any other factors specific to their business model, operations, or market that could impact the risk of ML, TF, or PF activities. These factors should be analysed and reflected in the BRA to ensure a comprehensive understanding of all risks the business may face.

3. Assessing and Understanding the Identified Risks

Once the inherent risks are identified, RPs must assess the likelihood and impact of these risks or the potential impact should they occur, using a structured methodology (e.g., risk matrix or heat maps), leveraging qualitative and quantitative data. Each risk factor such as prior STRs, compliance breaches, or audit findings may be useful indicators of risk exposure.

RPs are expected to assess each risk category independently and assign appropriate risk ratings (e.g., low, medium, high), justifying their conclusions with evidence and documented rationale. Where higher risks are identified, the RP must take enhanced measures to mitigate these risks.

4. Evaluating Controls

After assessing the inherent risks and associated vulnerabilities, RPs must evaluate the effectiveness of the controls and measures in order to mitigate these risks. This evaluation should be comprehensive, objective, and evidence-based, and should cover the following key areas:

- **AML/TFS Policies and Procedures**: Policies and procedures must be clearly documented, consistently implemented, and aligned with the ADGM AML Rulebook. They should reflect the firm's risk profile and ensure compliance with all applicable regulatory requirements
- **Customer Due Diligence ("CDD") Processes:** A robust CDD and Enhanced Due Diligence ("EDD") framework should be in place, ensuring that high-risk clients undergo thorough checks. This should include the collection of appropriate documentation, background checks, verification processes and ongoing monitoring to detect any suspicion.
- **Training and Awareness**: Staff must receive regular, at lease annual, AML/TFS training tailored to their roles and responsibilities. Training should equip employees with the knowledge needed to understand the firm's policies and procedures and effectively identify and escalate suspicious transactions or activities.

The assessment of control effectiveness should be objective and evidence based. The level of inherent ML/TF/PF risk should influence the type and levels of AML/TFS resources, controls and risk mitigation strategies, ensuring they are proportionate to the risks identified.

5. Determining Residual Risks

Following the control effectiveness evaluation, RPs must determine the residual risk, which refers to the level of risk remaining after all mitigating controls and measures have been applied. Residual risk ratings must be clearly defined and documented, and RPs must ensure that high residual risks are subject to enhanced monitoring and additional mitigation measures. This may include increased frequency of reviews, more intensive due diligence, senior management oversight, or targeted training for staff.

6. Documentation and Review

The BRA must be fully documented in a clear, structured, and accessible format. The documentation must describe the methodology used, the risk factors considered, the rationale for all risk ratings, the corresponding mitigation strategies and a summary of residual risks.

It is expected that the BRA be updated on a regular basis, at least annually, or more frequently in response to trigger events such as development of new products, business practices and technologies, update of the UAE NRA (including PF NRA), amendments to applicable regulation, significant changes to the business model or where a Firm becomes aware that a new ML/TF/PF risk has emerged, or an existing one has increased. The RPs must maintain proper version control and record of board or senior management approvals.

RPs are reminded of the AML and TFS obligations and regulatory expectations to ensure compliance with Federal AML/TFS Legislations, National Directives, the ADGM AML Rulebook and its regulatory expectations issued through notices to avoid any regulatory actions.

Sincerely,

Financial & Cyber Crime Prevention