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 ADGM Relevant Persons (RPs) including Financial Institutions (FIs), Virtual Assets Service Providers (VASPs) and Designated Non-Financial Businesses and Professions (DNFBPs), 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 RPs 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. ADGM 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 RPs' 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. RPs should differentiate/distinguish between ML, TF, and PF risks and assess them across the following core categories:

- **Customer Risk**: Evaluate the customer profile (individuals, legal persons, VASPs), geographical origin, industry, business practices, ownership structure, and classification as high-risk (e.g., politically exposed persons (PEPs) or non-residents).
- **Geographic Risk**: Assess exposure by jurisdictions where clients/counterparties reside, operate or transact; give heightened scrutiny to Jurisdictions non-compliant with international AML/TFS standards or identified as high-risk by international bodies such as FATF.
- **Product and Service Risk**: Assess risks inherent to products and services (e.g., anonymity, complex structures, rapid movement of funds or Dual-Use Good) that may increase exposure to ML/TF/PF.
- **Delivery Channel Risk**: Assess delivery methods (non-face-to-face onboarding, digital platforms, intermediaries, or agents). Channels that reduce verification or increase intermediate activity raise risk and require enhanced controls.
- **Transactional Risk**: Evaluate transaction size, frequency, volumes, patterns and complexity. Unusual, high-volume, or profile-inconsistent transactions particularly those involving high-risk jurisdictions should trigger heightened scrutiny.
- **New Developments and Technologies**: Assess risks from new products and technologies (cryptocurrency, blockchain, Artificial Intelligent (AI), or Machine Learning (ML), including features like anonymity, cross-border transactions, and strong encryption that could facilitate ML/TF/PF if not properly managed.
- **Emerging ML/TF/PF Risks:** Maintain systems and controls to identify, assess and promptly incorporate emerging or escalating ML, TF, and PF risks into the BRA ensuring timely mitigation appropriate measures.
- **Any other relevant factors specific to the business:** Consider any additional business- specific factors operational, structural or product-related that could impact the risk of ML, TF, or PF activities. Analysed and document these in the BRA to ensure a comprehensive risk assessment.

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**: Maintain clearly, well-determined policies and procedures that are consistently applied and aligned with the ADGM AML Rulebook. reflecting on the firm's risk profile and ensuring compliance with all applicable regulatory requirements.
- **Customer Due Diligence ("CDD") Processes:** Implement a robust CDD and Enhanced Due Diligence ("EDD") framework to ensure high-risk clients undergo thorough checks including collection of appropriate documentation, background verification and ongoing monitoring to detect any suspicion.
- **Training and Awareness**: Provide role-specific AML/TFS training to all staff at lease annually, ensuring employees understand the firm's policies and procedures and can 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/determine the type and intensity of AML/TFS resources, controls and mitigation measure, 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 Business Risk Assessment (BRA) be documented, proportionate to the nature, scale and complexity of the business and reviewed, updated regularly, at least annually, 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 RP becomes aware that a new ML/TF/PF risk has emerged, or an existing one has increased (AML Rules 4.1.1, 6.1.1 and 6.2.1). The RPs must maintain proper version control and record of board or senior management approvals for BRA versions.

All ADGM Relevant Persons (RPs), consisting of FIs, VASPs and DNFBPs, 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 supervisory guidance to avoid any regulatory actions.

Sincerely,
Financial & Cyber Crime Prevention