National Anti-Money Laundering and Combating Financing of Terrorism and Financing of Illegal Organizations Committee

United Arab Emirates

Suspicious Activity and Transaction Reporting Thematic Review

ABSTRACT

This thematic review sets out key findings and regulatory expectations based on the outcomes of the 2022 AML/CFT Examination conducted on Licensed Financial Institutions (LFIs) and Designated Non-Financial Businesses and Professions (DNFBPs) regarding Suspicious Transaction / Activity Reporting Framework.

Supervisory Authority Sub-Committee

January 2023

Defenitions

LFI	Licensed Financial Institution
ML	Money Laundering
DNFBPs	Designated Nonfinancial Businesses and Professions
TF	Terrorism Financing
PF	Proliferation Financing
AML/CFT	Anti-Money Laundering and Counter Financing Terrorism
KYC	Know Your Customer
STR	Suspicious Transactions Report
SAR	Suspicious Activity Report
Crime	As per Article 1 of the AML-CFT Law – Crime is defined as “money laundering crime and related predicate offences, or financing of terrorism or illegal organizations.”
Alerts	“Alerts” shall be understood to include automated transaction monitoring alerts, employee referrals, and law enforcement requests.
MLRO	Money Laundering Reporting Officer
SOP	Standard Operating Procedure
TM	Transaction Monitoring
TMS	Transaction Monitoring System
EDD	Enhanced Due Diligence
PEP	Politically-Exposed Person
CIF	Customer Information File
MIS	Management Information System
CRA	Customer Risk Assessment
FIU	Financial Intelligence Unit
MI	Management Information
TAT	Turnaround Time

Table of Contents

1. Introduction

1.1. Purpose

The purpose of this thematic review is to guide LFIs, DNFBPs and VASPs in understanding and effectively performing their statutory obligations under the legal and regulatory frameworks in force in the United Arab Emirates (UAE). This report was prepared based on the findings of the thematic desktop reviews conducted by the supervisory authorities, followed by validations performed during the 2022 full scope examinations with regards to TMS and STR Reporting Frameworks. It should be read in tandem with the Guidance for Licensed Financial Institutions On Suspicious Transaction Reporting (issued by Notice 3354/2022 dated 16/08/2022), the Guidance For Licensed Financial Institutions On Transaction Monitoring And Sanctions Screening (issued by Notice 4368/2021 dated 13/09/2021), and Supervisory Authorities Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations Guidelines for Financial Institutions (Notice 3090/2021) and any amendments or updates thereof . This review neither constitutes additional legislation nor regulation nor does it replace or supersede any legal or regulatory requirements or statutory obligations, but rather it sets out the standards of the supervisory authorities for LFIs and DNFBPs in relation to compliance with applicable TMS and STR requirements.

1.2. Applicability

Unless otherwise noted, the result of this Thematic Review applies to all natural and legal persons, which are licensed and/or registered by the Supervisory Authorities in the UAE, in the following categories:

1. National banks, branches of foreign banks, exchange houses, finance companies, payment service providers, registered hawala providers;
2. Insurance companies, agencies, and brokers;
3. Designated Non-Financial Business and Professions (DNFBPs);
4. Financial Institutions under the supervision of the Securities and Commodities Authority; and
5. Virtual Assets Service Providers.

1.3. Legal Basis

The Thematic Review conducted in 2022, builds upon the provisions of the following laws and regulations:

I. Federal Decree-Law No. (14) of 2018, Regarding the Central Bank & Organization of Financial Institutions and Activities, and its amendments (“CBUAE Law”);
II. Federal Decree-Law No. (20) of 2018 on Anti-Money Laundering (“AML”) and Combatting the Financing of Terrorism (“CFT”) and its amendments (“AML-CFT Law”);
III. Cabinet Decision No. (10) of 2019, as amended by Cabinet Decision No. (24) of 2022, Concerning the Implementing Regulation for Decree-Law No. (20) of 2018 on AML and CFT and Financing of Illegal Organisations (“AML-CFT Decision”) and its amendments;
IV. Cabinet Decision No. (74) of 2020 Regarding Terrorism Lists Regulation and Implementation of United Nations Security Council (UNSC) Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing, Countering the Proliferation of Weapons of Mass Destruction and its Financing and Relevant Resolution (“Cabinet Decision 74”), and its amendments;
V. Cabinet Decision No. (58) of 2020 regulating the Beneficial Owner Procedures (“Cabinet Decision 58”).
VI. ADGM Anti-Money Laundering and Sanctions Guidance and Rules (“AML Rules”)
VII. DFSA Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Module (“AML Rulebook”)

.

2. Regulatory Expectations, Acceptable Practices and Deficient Practices

2.1. Governance and Management Oversight

Expectations
• The LFI/DNFBP's compliance program should be appropriately funded, staffed, and equipped to effectively identify and report suspicious activity; • The LFI/ DNFBP's Senior Management must maintain a clear and sound tone from the top .The Board of Directors should ensure that the compliance program is prioritized within the organization. • Senior Management responsible for the compliance program should have sufficient authority, information access, and resources to ensure the reporting obligations on suspicious activity/transaction is carried out successfully. • Between the Board of Directors and Senior Management or as is in the case of DNFBPs, the interaction should be periodic whereby updates are shared (mainly from the Senior Management to the Board of Directors or equivalent in the case of DNFBPs) on the execution of the compliance program and its overall operational STR/SAR framework (that includes reporting metrics, technological- and process-related aspects). • The Compliance Officer or the Money Laundering Reporting Officer (MLRO) is accountable for reviewing, scrutinizing, and reporting STRs/SARs. The Compliance framework should ensure MLRO has an appropriate level of seniority, experience and independence to act in the role, with responsibility for implementation and oversight of its compliance; • The Compliance Officer or the MLRO responsibilities include but are not limited to the following: ➢ The detection of transactions related to any crime as defined in Article 1 of the AML-CFT Decision and subsequently reporting the associated suspicions to the FIU. ➢ Consistently conduct training sessions for all staff, particularly the first line of defense, to improve the frequency of reported internal SAR or STR. Ensuring that the utilized compliance program is risk-based and robust enough to manage current and emerging risk typologies.

Acceptable Practices	Deficient Practices
• Establishing a formal and documented reporting mechanism to inform the Board of Directors (or a relevant sub-committee of the Board or equivalent body in the case of DNFBPs) along with Senior Management on matters pertaining to compliance initiatives, compliance deficiencies and subsequent corrective actions, STRs, SARs, or other regulatory reports. The compliance program being prioritized within the organization supported by an effective identification, escalation, and reporting hierarchy.	Lack of managerial oversight via MI reports which led to the lack of coverage of critical components of LFIs and DNFBPs AML/CFT programs; example of such lapses include: • Lack of seniority and independence of the MLRO • Inconsistent tracking of alerts at each stage of the review along with the associated TATs. • Gaps identified in the TMS, future actions plans, etc.; • Number of STRs filed and emerging risk typologies observed; • Issues surrounding the implementation of the TMS and any progress updates to remediate those issues. • Lack of any training statistics on the STR/SAR framework. • Lack of managerial engagement also caused for limited resources to be allocated for TM alerts reviews or similar process in case of manual processes and related STR/SAR reporting to the FIU.

2.2. Policies and Procedures

Expectations

- LFIs and DNFBPs should have policies and procedures in place that govern changes to their AML/CFT compliance program. A robust process universe should help to ensure that such changes are defined, managed, controlled, reported, and audited.
- The AML/CFT compliance program should be in writing and include policies, procedures and controls that are designed to prevent, detect and deter money laundering and terrorist financing, including how LFIs/DNFBPs will determine high-risk operations associated with the products, services, delivery channels, customers and geographic locations; and provide for an AML/ CFT compliance program tailored to manage risks.

In addition, LFIs and DNFBPs should develop procedures for the investigation and processing of TM alerts through automated or manual process in order to file an STR and SAR reports promptly; the escalated reports should be comprehensive and ideally containing actionable information. The policies and procedures should cover the key processes for drafting and filing an STR/SAR. On a compliance-level, policies and procedures need to manage key AML/CFT risks and create an effective controls environment within the LFI/DNFBP.

Acceptable Practices	Deficient Practices
• LFIs and DNFBPs having documented formal policies and procedures which are reviewed and updated in line with the current and applicable regulations; • Ensuring that the up-to-date policies and procedures are communicated to the relevant staff. • Assigning clear accountability to staff for performance of duties under the AML/CFT program and establish clear accountability lines to ensure that there is appropriate and effective oversight of staff who engage in activities which may pose a greater AML/CFT risk. • Provide sufficient controls and monitoring tools for the timely detection and reporting of potentially suspicious activity, large transaction reporting and Cash transaction reporting. This should also include a procedure for recording the rationale for not reporting activity as a result of the findings of any investigation.	No adequate gap analysis conducted to ensure the policies and procedures are up-to-date and in line with the most recent AML/CFT Laws, Cabinet Decisions and Supervisory Authorities Guidelines; Weaknesses in the **Standard Operating Procedure** SOP for TM alert reviews, internal and external STR reporting processes. SOPs not being comprehensive enough to give clear directions to the relevant staff on the mitigation of AML/CFT risks coupled with a clear TAT for: • Dispositioning of automated and manual alerts/cases; • Compliance Officer or the MLRO's decisioning on whether to report a STR/SAR to the FIU; • Post-STR/-SAR mitigation actions. • Lack of reporting suspicious activity, and not including the description of how and to whom concerns should be raised, the role of the compliance officer / MLRO and what the "tipping off" restriction means in practice. • Lack of red flags and indicators in the SOP to identify potential suspicious activity. • Lack of sufficient KYC/CDD information and customer profile to facilitate transaction monitoring on ongoing basis for continued relationships.

2.3. Risk-Based Deployment of Transaction Monitoring Controls

Expectations

TM systems and processes should include:

- **Manual processes**, such as manual reporting and escalations by LFI/DNFBP employees, manual reviews of documentary-based transactions, manual adverse news screening, and discrepancies noted during periodic- or trigger event-based CDD reviews; and
- **Automated tools (where applicable)**, such as rule- or scenario-based automated suspicious activity monitoring systems, automated fraud detection systems, trade surveillance systems, TF and PF Screening Systems and automated adverse news screening tools.

LFIs and DNFBPs should firstly maintain a TM program based on an underlying AML/CFT risk-based assessment. The TM program should take into account the AML/CFT risks of the LFI/DNFBP's customers, prospective customers, counterparties, businesses, products, services, delivery channels, and geographic markets. Additionally, the components of the TM program should be able to prioritize high-risk alerts.

- LFIs and DFNBPs with a larger scale of operations are expected to have in place automated systems capable of handling the risks from an increased volume and variance of transactions. LFIs and DFNBPs utilizing automated systems should:
  - Perform a typology assessment to design appropriate rule- or scenario-based automated monitoring capabilities and processes. This should include risks outlined in the National Risk Assessment and other typology reports circulated by the Supervisory Authorities.
  - Employ quantifiable parameters that are tailored to the institution's risk profile and the specific product, service, and customer types involved in the transaction.
  - Implement risk-based customer and product segmentation, so that rule parameters and thresholds are appropriately calibrated to the type of activity subject to TM.
  - Utilize statistical tools or methods such as above-the-line and below-the-line testing; this involves increasing and decreasing the pre-determined thresholds of TM rules in a testing environment and measuring the resulting output to better fine-tune their calibrations and reduce the volume of false-positive alerts.
  - Where automated systems are employed, LFIs and DNFBPs should perform pre-implementation testing of TM systems using historical transaction data, as appropriate.
  - System testing should cover compatibility of the TM and core (source) systems with each other and with the overall AML/CFT and sanctions compliance infrastructure. Such testing is to ensure that the system performs as intended.

- While smaller LFIs and DNFBPs may rely on less sophisticated automated TM systems or manual processes, they should still ensure that they invest in appropriate tools to detect money laundering, terrorist financing and proliferation financing risks and identify potential outliers or deviations from the normal policy that may need to be reviewed.

Regardless of whether automated or manual processes (or a combination of the two) are used to perform TM, it is the LFI/DFNBP's responsibility to demonstrate that the monitoring program is effective and fit-for-purpose.

Acceptable Practices	Deficient Practices
• Implementation of a hybrid TMS incorporating both automated and manual processes depending on the size and complexity of the institution; • Implementation of Pre-transaction checks like Payment Screening for TF, PF and Sanction checks; • Automated tools' inclusion of rule- or scenario-based automated suspicious activity monitoring systems (which typically perform post-execution batch screening of transactions on a daily, weekly, monthly, and/or ad hoc basis); • Manual tools' inclusion of unusual activity or unusual transactions being reported by the first line of defense customer-facing staff; an example of such reporting would be internal whistleblowing incident. • Large LFIs/DNFBPs performing pre-implementation testing of TM systems, using historical transaction data. • The internal technology or tool deployed by the LFI and DNFBP is in line with the regulated entity's AML/CFT program, is functioning as intended and within the	• DNFBPs not maintaining internal monitoring tools or manual processes in place to detect ML/TF risks. • The LFIs and DNFBPs did not perform any typology assessment, which covers red flags that are relevant to their operations. These assessments are designed to help build appropriate rule- and scenario-based automated monitoring capabilities and/or manual processes; • LFIs and DNFBPs did not design customized detection scenarios and parameters that are relevant to their operations; • Utilization TM scenarios which are not risk-based (disproportionate to the risk) – an example would be customer risk levels (Low/Medium/High) not being considered while setting up the thresholds for each detection scenario. This would suggest that LFIs and DNFBPs would monitor customers with varying risk levels using the same thresholds; • LFIs not performing risk-based customer segmentation to create risk groups, based on their profile and nature of

predefined parameters. • Small scale DNFBPs developing an effective manual transaction monitoring process by effectively utilizing resources	business. In doing so, the LFIs and DNFBPs could not anticipate expected transactional activity in an effort to apply appropriate thresholds to respective customer segments; • LFIs not performing adequate statistical analysis to apply thresholds and parameters for detection scenarios. Additionally, not maintaining a documented methodology for threshold fine-tuning; LFIs not having sufficient knowledge and dedicated resources to perform TM model testing and validation. Overall, failing to implement adequate thresholds for the different risk levels identified, as part of the CRA, impedes the LFI/DNFBP's ability to flag, investigate, and report unusual transactions. DNFBPs not prioritizing high risk clients while conducting transaction monitoring to apply a risk based approach

2.4. Data Identification and Management

Expectations	
• LFIs and DNFBPs should identify and document all data sources that serve as inputs to their TM program, including internal customer databases, core- system, or other transaction processing systems, and external sources such as SWIFT message data; • Where automated TM systems are used, LFIs and DNFBPs should institute data extraction and loading processes to ensure complete, accurate, and traceable data flows from their source to the TMS; • Both prior to initial deployment and at risk-based intervals thereafter, LFIs and DNFBPs should test and validate the integrity, accuracy, and quality of data to ensure that accurate and complete data is flowing into the TMS; • Data testing and validation should typically occur every 12 to 18 months or earlier as deemed appropriate based on the outcomes the ML/TF risk assessment, risk appetite and any ad-hoc internal and external factor(s). Moreover, the frequency of such activities should be clearly documented; • Such testing can include data integrity checks to ensure that data is being completely and accurately captured in source systems and transmitted to the TMS, as well as to ensure the reconciliation of transaction codes across core systems and TMS; • LFIs and DNFBPs should place appropriate detection controls, such as the analysis of trends observable through management information. They should also generate exception reports in order to identify abnormally functioning TM rules or scenarios; Any identified irregularities caused by data integrity or other data quality issues should be escalated to Senior Management and must be remediated in a timely manner.	
Acceptable Practices	**Deficient Practices**
Most of the LFIs and DNFBPs having data integrity and accuracy check processes in place, to ensure all relevant customer and transactional data are flowing into TM. DNFBPs having appropriate internal systems to maintain adequate KYC/CDD and transactional data to facilitate ongoing transaction monitoring through automated or manual process	• Inconsistent and incomplete customer data in the core-systems and/or other relevant systems; • Multiple customer information file (CIF) and risk ratings for the same customer; • No documented process for data integrity and accuracy checks to provide clear directions to both first line of defense and second line of defense in terms of the roles and responsibilities, frequency, TAT, escalation/approval matrix. • No adequate detection controls mechanism ("trigger events"), such as the analysis of trends observable through MI data as it pertains to alerts, cases and STR volumes, trends and patterns and the generation of exception reports, to identify abnormally functioning TM rules or scenarios.

2.5. Alert Review, Case Investigation, and STR or SAR Decision Making

Expectations

- An efficient alert (automated or manual) management and disposition process is essential to safeguarding the financial integrity of LFIs and DNFBPs, assisting law enforcement in the identification and investigation of criminal activity, and satisfying regulatory expectations concerning timely suspicious activity reporting. The alert management and dispositioning process should be adequately staffed and should include a process for the expedited filing of urgent reports for select cases.
- The LFI and DNFBPs should apply a risk-based approach to the alert review process or as applicable to DNFBPs through the manual process by prioritizing alerts based on their risk category. In other words, alerts generated on suspicious transactions of higher-risk customers should be risk scored accordingly and prioritized for review.
- Alert Review: LFI/DNFBP's employees should review an alert and determine whether further investigation is warranted. The underlying basis for the determination should be documented in accordance with the LFI/DNFBP's investigation procedure.
- Where the facts available at the alert review stage are or may be sufficient enough to warrant an STR or SAR filing without further investigation, or where the transaction may otherwise require immediate attention, employees should immediately escalate the alerted activity to the designated STR or SAR decisioning authority (i.e. the Compliance Officer or the MLRO in this case) for expedited review.
- Case Investigation: For any alerted activity deemed to require further investigation, employees should conduct and complete (at least preliminary) an investigation of the alerted activity, document the results of any research or analysis performed, and make a recommendation as to whether an STR or SAR should be filed.
- Where a case investigator becomes aware of activity that requires immediate attention, employees should immediately escalate the activity to the designated STR or SAR decisioning authority (i.e. the Compliance Officer or the MLRO in this case) for expedited review. The Compliance Officer or MLRO must maintain records of decisions made.
- In the event of escalation for expedited review, the Compliance Officer or the MLRO should review the activity and make a determination as to whether or not it is suspicious within 24 hours from the time of escalation and should file an STR or SAR to the FIU accordingly. Where appropriate, the Compliance Officer or the MLRO should also escalate the activity for potential exit, account closure, and internal watchlist addition.
- The LFI/ DNFBPs needs to evaluate continuing the relationship (except in the cases related to Narcotics / terrorism) with the customer by placing enhanced monitoring controls based on the nature of concern and their own risk appetite;
- In the absence of escalation for expedited review, LFIs are expected to file an STR/SAR within a maximum of 35 business days from the date of alert generation.

Acceptable Practices	Deficient Practices
• LFIs and DNFBPs having defined a clear escalation and investigation framework for investigation of alerts, raising internal STRs) and reporting STRs/SARs to FIU. • Most of the LFIs have a defined and clear TAT for each stages of alert clearance and reporting process and post-STR mitigation activities. • Most of the LFIs and DNFBPs have case management system to record, review, and escalate TM alerts. • DNFBPs having written procedures defining the role of front end staff, MLRO and Senior Management for identifying and reporting potential suspicious activity. • Having adequate knowledge about regulatory obligations, red flags and typologies by the relevant staff in order to raise internal STR/SAR.	• No alert risk-scoring model for prioritizing alerts. The prioritization of alerts is done manually with no documented methodology or approach for risk-based alert allocation or prioritization; • The alert closure comments, for both automated and manual alerts internal STRs, are too generic and do not effectively articulate the underlying ML/TF and PF risk. The disposition does not explain/discount the initial red flag/s identified in the system and by the first line of defense; • No evidence of adverse media/sanctions/PEP-screening on the counterparty(s) in the TMS and in the alert/case closure comments; • No standard approach and documented process for adverse media screening as part of the TM alert review; • The counterparties involved are not adequately analyzed or documented in the case closure comments; • Supporting documents, in relation to alert/case review, are not attached in the TMS; • Inconsistency in recording and reviewing the internal STRs received from other departments; • Lack of maintenance of an adequate tracker or log for the cases that have been escalated by employees to the Compliance Officer or the MLRO and their final outcomes; • Lack of maintenance of an adequate tracker or log for recording internal STRs; • The Compliance Officer or the MLRO's decision whether

	to close the case or report an STR/SAR to the FIU is not clearly documented; • Delays in clearing the alerts and reporting STRs/SARs to the FIU; • LFIs and DNFBPs not having case management workflow functionality to review and escalate TM alerts; • The documents related to alerts/cases/STRs not being stored in a single repository. • DNFBPs not differentiating between STR/SAR and other reporting types such as DPMS Report and Real Estate Activity Report • Customers rejected while onboarding stage due to potential suspicious activity not evaluated as potential SAR (attempted transactions)

2.6. Post STR and SAR Process

Expectations	
• Once a suspicious transaction or other suspicious information related to a customer or business relationship has been reported to the FIU, the LFIs and DNFBPs should take the following immediate actions: ➢ LFIs and DNFBPs should follow the instructions, if any, of the FIU in relation to both the specific transaction and to the business relationship in general. ➢ In cases where the institution hasn't received any response/query from the FIU, the institution needs to put in place adequate controls like Enhanced due diligence and on-going monitoring activity in line with their own Risk Appetite; ➢ LFIs and DNFBPs should identify all related/associated accounts or relationships of STR or SAR customers and conduct a review on those accounts/relationships to check whether any suspicious transaction(s) has taken place. If yes, appropriate risk-based Enhanced Due Diligence ("EDD") and ongoing monitoring procedures should be implemented. ➢ The customer or business relationship, including the related/associated accounts and relationship to the STR or SAR customers, should immediately be classified as high-risk and appropriate risk-based EDD and ongoing monitoring procedures should be implemented in order to mitigate the associated ML/TF risks. Unless specifically instructed by the FIU to do so, LFIs and DNFBPs are under no obligation to carry out transactions they suspect, or have reasonable grounds to suspect, of being related to a crime. Furthermore, unless specifically instructed by the FIU to maintain the business relationship (for example, so that the competent authorities may monitor the customer's activity), it should be the LFI's responsibility to take appropriate steps in order to decide whether or not to maintain the business relationship based on their risk appetite. Commensurate with the nature and size of their businesses, LFIs and DNFBPs that decide to maintain the business relationship should: ➢ Document the process by which the decision was made to maintain the business relationship, along with the rationale for, and any conditions related to, the decision; and ➢ Implement adequate EDD measures to manage and mitigate the ML/TF risks associated with the business relationship, including but not limited to, ensuring the STR or SAR subject is added into the relevant lists for close monitoring such as internal watchlists/blacklists, changing the customer risk rating, etc.; ➢ Obtain approvals from the relevant compliance and business stakeholders; ➢ Ensure that the customer is not tipped off about any SAR or STR reported by LFIs and DNFBPs.	
Acceptable Practices	**Deficient Practices**
LFIs and DNFBPs having documented Standard Operating Procedure (SOP) for post-STR process (i.e. exit procedure, adding the names into internal watch list, increasing the risk rating to "High" post STR, if the LFI/DNFBP decided to retain the relationship).	• No adequate procedures and mechanism to identify all related or associated accounts or relationship of STR or SAR customers and conduct a review on those accounts/relationships to check whether any suspicious transaction(s) has taken place; • For relationship retained customers – Post-STR, customer or business relationship is classified as a high-risk customer; • For relationship exited customers – Post-STR, customer or business relationship is classified as a high-risk customer;

	• No adequate rationale is documented for retaining relationship, post-STR; • Inconsistency in adding the STR or SAR subject and other related or associated parties into the relevant list for close monitoring or internal watchlists/blacklists.