



# **CBUAE OUTREACH EVENT on the AML/CFT Guidance for LFIs on Transaction Monitoring and Sanctions Screening**

14 September 2021

## Outline of this Presentation

- Purpose, Applicability, and Structure of the Guidance
- Operational Lifecycle of TM and SS Systems
  - Risk Assessment and Risk-Based Design of Controls
  - Data Identification and Management
  - System Specifications and Pre-Implementation Testing
  - Operational Issues and Maintenance
  - Outcomes Analysis and Reporting
  - Post-Implementation Testing, Tuning, and Validation
- Program Governance and Oversight
- Q & A

# Purpose & Applicability of the Guidance Document

## Purpose

- This Guidance does NOT constitute new regulation and does NOT introduce new legal obligations.
- It is designed to help CBUAE's LFIs understand the purpose and context of their existing legal obligations, as well as the CBUAE's expectations for how those obligations will be fulfilled.
- The Guidance came into effect on 13 September 2021, with LFIs expected to demonstrate compliance with its requirements within one month from its coming into effect.

## Applicability

The guidance document applies to **all natural or legal persons that are licensed and/or supervised by the CBUAE** in the following categories:

- National banks, branches of foreign banks, exchanges houses, finance companies, and other licensed financial institutions ("LFIs"); and
- Insurance companies.

## Additional Guidance Related to TM and SS

LFIs should also consult the following guidance documents, which set forth additional supervisory expectations and guidance related to TM and SS:

- With respect to TM, LFIs should also consult the CBUAE's *Guidance for LFIs on Suspicious Transaction Reporting*; and
- With respect to SS, LFIs should also consult:
  - The Executive Office of the Committee for Goods and Materials Subjected to Import and Export Control's *Guidance on TFS for Financial Institutions and Designated Non-financial Business and Professions*; and
  - The CBUAE's *Guidance for Licensed Financial Institutions on the Implementation of TFS*.

# Structure of the Guidance and This Presentation

- The Guidance is divided into separate sections on transaction monitoring (“TM”) and sanctions screening (“SS”).
- Each section is organized around the **operational lifecycle** of the respective controls—from initial risk assessment and system design, to pre-implementation testing and deployment, through to outcomes analysis and post-implementation testing, tuning, and validation.
- This presentation follows that operational lifecycle for both TM and SS systems **in parallel**, discussing the distinguishing features of each set of controls along the way, as applicable.
- The presentation concludes with a discussion of appropriate **governance and oversight** for an LFI’s TM and SS programs as a whole, including training, management reporting, and auditing.



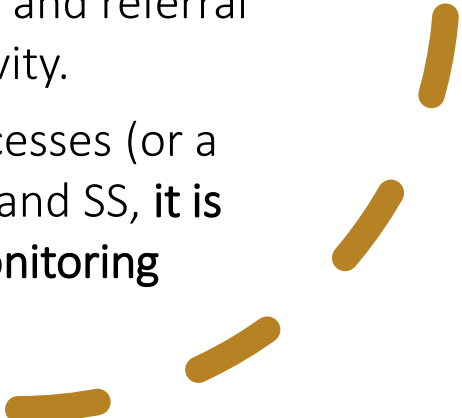
- The design of an LFI's TM and SS programs should be informed by the LFI's **enterprise risk assessment**, so that relevant and effective controls are applied across the full range of risks to which the institution is exposed and enhanced scrutiny is applied to the areas of highest risk.
- An LFI's risk assessment should include, at a minimum, an assessment of the **customers, products and services, delivery channels, and geographic exposure** presenting the greatest money laundering ("ML"), terrorist financing ("TF"), and proliferation financing ("PF") risks.
- The risk assessment should also include an assessment of the **strength of the controls** currently in place to mitigate these risks, and allow for an assessment of the residual risk that remains after accounting for the effectiveness of controls.



# Risk Assessment



# The Risk-Based Approach to TM and SS

- An LFI's TM and SS programs should be tailored to the ML/TF/PF risks of its customers and business activities, and calibrated to the size, nature, and complexity of the LFI.
    - **LFIs 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.
    - While **smaller LFIs may rely on TM and SS systems that are less automated**, they should still ensure that these are appropriately executed to address the risks from their day-to-day transactional activity.
    - Additionally, **all SS systems should be fully automated for the update of any changes to the UN Consolidated List and the Local Terrorist List.**
  - Particularly where purely manual processes are employed, LFIs should implement **appropriate training** to ensure that personnel adhere to the internal processes for identification and referral of potentially suspicious or sanctions-related activity.
  - Regardless of whether automated or manual processes (or a combination of the two) are used to perform TM and SS, **it is the LFI's responsibility to demonstrate that the monitoring program is effective and appropriately risk based.**
- 

## Overview of TM and SS Systems and Processes

### Transaction Monitoring

Transaction monitoring systems and processes can include:

- **Manual processes**, such as manual reporting and escalations by LFI employees, manual reviews of document-based transactions, manual negative news screening, and periodic or event-based CDD reviews; and
- **Automated tools**, such as rule- or scenario-based automated suspicious activity monitoring systems, automated fraud detection systems, trade surveillance systems, and automated negative news screening tools.

### Sanctions Screening

Similarly, sanctions screening systems and processes can include:

- **Manual processes**, such as manual reporting and escalations by LFI employees, manual reviews of document-based transactions, and periodic or event-based CDD reviews; and
- **Automated tools**, such as automated name screening tools that compare customer databases against applicable sanctions lists, transaction filtering tools that screen payment message and transaction data against applicable sanctions lists prior to execution, and text analytics tools that automatically convert paper documentation into electronic data that can then be screened against applicable sanctions lists.

This next several slides will focus primarily on *automated* TM and SS systems and processes, given their increased technical and operational complexity.



## Data Identification and Management

### Data Identification and Extraction

- LFI should **identify and document all data sources that serve as inputs** into their TM and SS programs, including internal customer databases, core banking or other transaction processing systems, and external sources such as SWIFT message data.
- Source system documentation should **identify a system owner or primary party responsible** for overseeing the quality of source data and addressing identified data issues.
- Where automated TM or SS systems are used, LFI should institute **data extraction and loading processes** to ensure a complete, accurate, and fully traceable transfer of data from its source to TM and SS systems.

### Testing and Validation of Source Data

- Both prior to initial deployment and at risk-based intervals thereafter, LFI should **test and validate the integrity, accuracy, and quality of data** to ensure that accurate and complete data is flowing into their TM and programs.
- Data testing and validation should typically occur at minimum **every 12 to 18 months**, as appropriate based on the LFI's risk profile, and 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 TM and SS systems, as well as the **reconciliation of transaction codes** across core banking and TM and SS systems.


### Data Issue Management

- LFI should put in place appropriate **detection controls**, such as the analysis of trends observable through management information system ("MIS") data and the generation of exception reports, **to identify abnormally functioning TM rules or scenarios or SS logic**.
- Any identified irregularities caused by data integrity or other data quality issues should be **escalated** to appropriate senior management and **remediated** in a timely manner.



# System Specifications: TM Rules




- LFI should employ **TM detection scenarios (or “rules”)** that are designed to identify potentially suspicious or illegal transactions and elevate them for further review and investigation.
    - LFIs utilizing automated systems should perform a **typology assessment** to design appropriate rule- or scenario-based automated monitoring capabilities and processes.
    - Transactions may be suspicious simply in virtue of their individual characteristics (such as their value, source, destination, or use of intermediaries) or because, together with other transactions, they form a pattern that is unusual or suspicious.
  - TM rules should employ value and other **thresholds and parameters** that are tailored to the institution’s risk profile and the specific product or service and customer type involved in the transaction.
    - LFIs should perform risk-based **customer and product segmentation**, so that rule parameters and thresholds are appropriately calibrated to the type of activity subject to TM.
    - LFIs with larger transaction volumes should consider employing **above-the-line and below-the-line testing** to better fine-tune their rules and reduce the volume of false-positive alerts.
  - In order to identify patterns of potentially suspicious activity spanning multiple transactions, LFIs should group individual TM parameters and thresholds into **multi-factor risk scenarios**.
    - Key typologies and associated indicators are included in the CBUAE’s *Guidance for LFIs on Suspicious Transaction Reporting*.
  - The use of scenarios should not be limited to LFIs with automated transaction monitoring systems, as **smaller institutions with less-automated systems can and should apply the same logic in training and guiding their staff to detect these more complex risks**.
  - In all cases, LFIs should maintain **documentation** that articulates the institution’s current detection scenarios and their underlying assumptions, parameters, and thresholds.
- 



# System Specifications: Name Screening




- The process of screening information collected and maintained by an LFI on the parties it does business with and their related parties is referred to as “**name screening.**”
  - Name screening encompasses any data set within the LFI’s operations, separate from its transaction records, that may present a relevant sanctions risk indicator or be conducive to detection through screening, including:
    - **Customer data**, including the names and addresses of existing or prospective customers, their beneficial owners, and other related or connected parties whose information is collected pursuant to risk-based due diligence procedures;
    - **Employee data**, including employee names and addresses;
    - **Third-party service provider data**, including the names, addresses, and beneficial owners of an LFI’s vendors, landlords, and tenants, as applicable;
    - **International Securities Identification Numbers** (“ISINs”) and other sanctions-relevant identifying features of assets held in custody by the LFI; and
    - **Recipients of the LFI’s corporate donations or sponsorship.**
  - Name screening (whether automated or manual) must be performed prior to the onboarding of a customer and/or the facilitation of an occasional transaction and on an ongoing basis (at least daily) thereafter.
- 



# System Specifications: Transaction Screening



- The process of screening a movement of value—including funds, goods, or assets—out of, into, or through the LFI between parties or accounts is referred to as “**transaction screening.**”
  - LFIs should screen all payments prior to completing the transaction, utilizing all transaction records necessary to the movement of value between parties, which may include:
    - The parties involved in a transaction, including the **originator and beneficiary**;
    - **Agents, intermediaries, and financial institutions** involved in a transaction;
    - **Bank names, Bank Identifier Codes (“BICs”), and other routing codes**;
    - **Free text fields**, such as payment reference information or the stated purpose of the payment in Field 70 of a SWIFT message;
    - **ISINs** or other risk-relevant product identifiers, including those that relate to sectoral sanctions identifications within securities-related transactions, as applicable;
    - **Trade finance documentation**; and
    - **Geographic details**, including but not limited to addresses, countries, cities, towns, regions, ports, and airports (e.g., as contained within SWIFT Fields 50 and 59 or acquired through vessel tracking inquiries).
  - Transaction screening should be performed at a point in time where a transaction can be stopped and thus before a potential violation occurs.
    - Particular attention should be directed to any points within the transactional process where relevant information could be changed, modified, or removed in order to undermine screening controls.
- 



# Pre-Implementation Testing

- Where automated systems are employed, LFIs should perform **pre-implementation testing of TM and SS systems**, using historical transaction data as appropriate.
- Such testing should include **system integration testing**, to ensure compatibility of the TM and SS systems with source systems and other AML/CFT and sanctions compliance infrastructure, and **user acceptance testing**, to ensure that the system performs as anticipated in the operating environment.
- Material data mapping, transaction coding, and other data quality issues, as well as irregularities in TM or SS model performance and outputs, identified through pre-implementation testing should be **prioritized for remediation and subject to re-testing** prior to the deployment of a TM or SS system.



# System Operation and Maintenance

# TM Alert Scoring and Prioritization

- Consistent with a risk-based approach, LFIs may consider assigning **risk-weighted scores** to TM alerts in order to prioritize higher-risk alerts for expedited review.
- LFIs may opt to assign a higher risk score, and thus to prioritize for review and investigations, transactions that violate **individual TM rules** corresponding with especially heightened risks (based on the risk profile and risk appetite of the institution) as well as transactions identified as violating **multiple TM rules**.
- LFIs with larger TM alert review and investigation teams may likewise opt to allocate higher-scoring alerts to more senior investigators or those with specialized expertise in certain risk areas.
- Although alert scoring may be used to achieve a risk-based prioritization and allocation of manually generated TM alerts, such processes may be especially useful for LFIs faced with a high volume of alerts produced by automated TM systems.

# Sanctions List Management

- Under Article 21.2 of Cabinet Decision 74, LFIs' sanctions screening lists must include all names on lists issued by the UNSC and its relevant Committees (**UN Consolidated List**) or by the UAE Cabinet (**Local Terrorist List**).
- In addition, LFIs' sanctions screening processes should include searches for entities that are not themselves listed but that are **owned or controlled mainly or fully by a listed person**.
  - Because such "**shadow designated persons**" are not listed by government authorities, LFIs should develop **internal lists** of such persons based on their own due diligence and consideration of external sources, and include such lists in their SS program.
- Given the dynamic nature of TFS, LFIs should establish and implement **sanctions list management procedures** that consider:
  - List selection;
  - Sourcing of lists;
  - List maintenance;
  - Data enhancement;
  - Whitelisting;
  - Geographic scope of application;
  - Exact matching versus "fuzzy logic; and
  - Frequency of screening.



## Outcomes Analysis and Management Information Systems Reporting

### Outcomes Analysis

- LFIs should **document and track TM and SS outputs** in order to identify and address any technical or operational issues and understand key risks or trends over time.
- Irregularities in TM or SS system performance, including significant changes in the productivity of TM rules or the volume of apparent matches to sanctions lists over time, may be indicative of **underlying data quality or data integrity issues** or of the **need to recalibrate rule thresholds or parameters or SS logic**.
  - Identified data quality or integrity issues should be reported back to designated data or owners, and apparent rule calibration issues (such as unproductive rules or those producing excessive volumes of false positive alerts) or screening logic issues should be reported back to model owners for tuning and optimization.
- For TM systems specifically, where outcomes analysis reveals that certain transaction types or patterns are repeatedly flagged by the TM system and then consistently cleared as false positives by TM investigators, the LFI may consider employing a risk-based **suppression logic or other “whitelisting” process** to prevent the generation of alerts on activity repeatedly deemed not to be suspicious.
  - Such methods, however, should not be applied to higher-risk customer or transaction types and should be carefully monitored and subject to periodic and event-driven testing, tuning, and validation, as described below.

### MIS Reporting

- LFIs should ensure that **senior management is regularly updated on the performance and output of their TM and SS programs**, including through the provision of metrics, trends, and other management information systems (“MIS”) reporting generated by TM or SS systems or produced by alert review and investigation teams.
- Such reporting may include an analysis of the number of alerts produced by each TM rule and the proportion of such alerts that are cleared as false positives, that require further investigation, and that ultimately result in the filing of an STR/SAR, as well as an analysis of the number and type of SS hits and the proportion of apparent matches that are cleared as false positives compared to those that are confirmed as potential or true matches.
- MIS reporting and analysis should feed back into an LFI’s financial crimes risk assessment, and LFI management should use this information to ensure that the institution’s customers and transaction remain within the LFI’s risk appetite.



# Post-Implementation Testing, Tuning, and Validation

- On a periodic basis and in the event of material system output or operational irregularities, **LFIs should reassess the functionality of TM and SS systems and processes**, including the continued relevancy of detection scenarios and the calibration thresholds, parameters, and screening logic.
  - Post-implementation testing should include checks for system integration, data quality, and operational functionality, and should include back-testing of TM rules to ensure their effectiveness.
  - Any proposed material adjustments to TM rules or SS search logic should be then subject to pre-implementation testing using sample or historical data to ensure their proper functioning, and should be reflected in updated documentation.
- **TM and SS model testing and validation** should be performed by individuals with sufficient expertise and appropriate level of independence from the model's development and implementation.
  - Generally, validation should be done by people who are not responsible for the development or use of the model and do not have a stake in whether a model is determined to be valid.
  - Independence may be supported by the separation of reporting lines or by the engagement of an external party not responsible for model development or use.
  - All model validation activities and identified issues should be clearly documented, and management should take prompt action to address model issues.

- The LFI's board of directors and senior management should exercise active oversight of the institution's TM and SS programs.
  - The board and senior management should ensure that there are effective TM and SS systems supported by adequate internal expertise and resources.
  - TM and SS functions should be given clear and distinct responsibilities for their respective tasks in the TM and SS process chain (e.g., for alert handling and the filing of STRs/SARs).
- LFIs are expected to implement effective reporting systems to ensure that their board and senior management are updated on key financial crimes risks in a timely manner.
  - Any data quality or system functionality or output issues should be documented and tracked, and the status of remedial actions should be reported regularly to senior management.
- TM and SS programs should be subject to independent testing by internal or external auditors with sufficient technological expertise and understanding of ML/TF/PF and sanctions risks and requirements.




# Oversight, Management Reporting, and Auditing



# Use of Vendors and Other Third Parties



- LFI's may use externally provided TM or SS services and other third-party providers to fulfil their legal and regulatory obligations to monitor and screen their customers and transactions. **However, LFI's are ultimately responsible for complying with AML/CFT and sanctions requirements, even if they choose to use third-party models to assist with their compliance obligations.**
  - **The selection of third-party system or service should be guided by the LFI's size, geographic footprint, business and technology environments, and financial crimes risks, as well as functional requirements,** such as the volume of data to be screened, the degree to which TM and SS processes will be centralized across business lines, the nature of existing data integrity processes, and the ability of the application to integrate effectively within an LFI's technological infrastructure.
    - When selecting a vendor, LFI's should require the vendor to provide developmental evidence explaining the product components, design, and intended use, so as to determine whether the model is appropriate for the LFI's products, exposures, and risks.
  - **LFI's are expected to validate their own use of vendor products.**
    - Vendor models are often designed to provide a range of capabilities and so may need to be customized by an LFI for its particular circumstances. An LFI's customization choices should be documented and justified as part of validation.
    - The LFI also should conduct ongoing monitoring and outcomes analysis of vendor model performance using the LFI's own outcomes.
    - It is also very important for the LFI to have as much knowledge in-house as possible, in case the vendor or the LFI terminates the contract for any reason, or if the vendor is no longer in business. LFI's should have contingency plans for instances when the vendor model is no longer available or cannot be supported by the vendor.
- 

# Role-Specific Training

- Personnel responsible for performing TM and SS roles should receive training that covers key financial crimes risks faced by the institution, complex and higher-risk customer and transaction types relevant to TM and SS processes, applicable legal and regulatory requirements, and internal policies, procedures, and processes.
  - Training should be **tailored to each individual's specific responsibilities** and include desktop procedures or instructions for the use of any TM or SS systems or other technology relevant to the individual's role.
  - An LFI's TM and SS training should be subject to **completion tracking and escalation** procedures to ensure timely completion of mandatory training by all relevant personnel.
  - Mandatory training should also be extended to any **staff located abroad** whose responsibilities cover accounts booked in or activity flowing into, out of, or through the UAE.



# Questions