مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM AND ILLEGAL ORGANISATIONS

GUIDANCE FOR LICENSED FINANCIAL INSTITUTIONS ON TRANSACTION MONITORING AND SANCTIONS SCREENING

September 8, 2021

Contents

1. Introduction

1.1. Purpose

Article 44.11 of the *Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations* charges Supervisory Authorities with "providing Financial Institutions…with guidelines and feedback to enhance the effectiveness of implementation of the Crime-combatting measures."

The purpose of this Guidance is to **assist** the understanding and effective performance by the United Arab Emirates Central Bank's ("CBUAE") licensed financial institutions ("LFIs") of their statutory obligations under the legal and regulatory framework in force in the UAE. It should be read in conjunction with the CBUAE's *Procedures for Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations* (issued by Notice No. 74/2019 dated 19/06/2019) and *Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations for Financial Institutions* (issued by Notice 79/2019 dated 27/06/2019) and any amendments or updates thereof.[1] As such, while this Guidance neither constitutes additional legislation or regulation nor replaces or supersedes any legal or regulatory requirements or statutory obligations, it sets out the **expectations** of the CBUAE for LFIs to be able to demonstrate compliance with these requirements. In the event of a discrepancy between this Guidance and the legal or regulatory frameworks currently in force, the latter will prevail. This Guidance may be supplemented with additional separate guidance materials, such as outreach sessions and thematic reviews conducted by the Central Bank.

Furthermore, this Guidance takes into account standards and guidance issued by the Financial Action Task Force ("FATF"), industry best practices and red flag indicators. These are not exhaustive and do not set limitations on the measures to be taken by LFIs in order to meet their statutory obligations under the legal and regulatory framework currently in force. As such, LFIs should perform their own assessments of the manner in which they should meet their statutory obligations.

This Guidance comes into effect immediately upon its issuance by the CBUAE with LFIs expected to demonstrate compliance with its requirements within one month from its coming into effect.

1.2. Applicability

Unless otherwise noted, this guidance applies to all natural and legal persons, which are licensed and/or supervised by CBUAE, in the following categories:

- National banks, branches of foreign banks, exchange houses, finance companies and other LFIs; and
- Insurance companies.

[1] Available at https://www.centralbank.ae/en/cbuae-amlcft.

1.3. Legal Basis

This Guidance builds upon the provisions of the following laws and regulations:

(i) Federal Decree-Law No. (20) of 2018 on Anti-Money Laundering ("AML") and Combatting the Financing of Terrorism ("CFT") and Financing Illegal Organisations ('AML-CFT Law");

(ii) Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation for Decree-Law No. (20) of 2018 on AML and CFT and Financing of Illegal Organisations ("AML-CFT Decision"); and

(iii) 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").

With respect to transaction monitoring ("TM"), and as per Articles 4.2 (a) and 20 of AML-CFT Decision, LFIs are obliged to develop internal policies, controls, and procedures that are commensurate with the nature and size of their business and are approved by senior management to enable them to manage the crime risks that have been identified. They must also continuously update them. Furthermore, under Article 16 of AML-CFT Decision, LFIs must put in place indicators that can be used to identify suspicious transactions and other activity in order to file suspicious transaction reports ("STR"), suspicious activity reports ("SAR") or other report types to the UAE's Financial Intelligence Unit ("FIU). LFIs must update these indicators on an ongoing basis, in line with all applicable instructions from the UAE's supervisory authorities and FIU.

With respect to sanctions screening, and as per Article 21.2 of Cabinet Decision 74, LFIs are obliged to regularly screen their databases and transactions against names on lists issued by the UNSC and its relevant Committees (UN Consolidated List) or by the UAE Cabinet (Local Terrorist List), and also immediately when notified of any changes to any of such lists. Such screening must include regular searches of their customer databases, parties to any transactions, potential customers, beneficial owners, and persons and organizations with which the LFI has a direct or indirect relationship. LFIs must also screen their customer database before conducting any transaction, or entering into a business relationship with any person, to ensure that their name is not listed on the UN Consolidated List or the Local Terrorist List.

For more details and information, please refer to the Executive Office of the Committee for Goods and Materials Subject to Import and Export Control's ("Executive Office") *Guidance on TFS for Financial Institutions and Designated Non-financial Business and Professions*[2], the CBUAE's *Guidance for Licensed Financial Institutions on the Implementation of TFS,* and the CBUAE's *Guidance for Licensed Financial Institutions on STR*[3]. LFIs should consult the CBUAE's and the Executive Office's websites as updated from time to time.

1.4. Acronyms

Terms	Description
AML	Anti-money laundering

[2] Available at: https://www.uaeiec.gov.ae/en-us/un-page.
[3] Available at: https://www.centralbank.ae/en/cbuae-amlcft.

CBUAE	Central Bank of the United Arab Emirates
CDD	Customer due diligence
CFT	Combating the financing of terrorism
FATF	Financial Action Task Force
FIU	Financial intelligence unit
ISIN	International Securities Identification Numbers
KYC	Know your customer
LFI	Licensed financial institution
MIS	Management information systems
ML	Money laundering
OCR	Optical character recognition
PF	Proliferation financing
SAR	Suspicious activity report
STR	Suspicious transaction report
SWIFT	Society for Worldwide Interbank Financial Telecommunications
TF	Terrorist financing
TM	Transaction monitoring
TFS	Targeted financial sanctions

2. Transaction Monitoring

An effective TM program enables LFIs to detect, investigate, and report suspicious transactions, in compliance with the UAE's legal and regulatory framework, and to ensure that the institutions' customers and transactions remain within their risk appetite. Effective TM therefore depends critically on information obtained through the application of customer due diligence ("CDD")/know your customer ("KYC") measures, including but not limited to information regarding the types of transactions in which the customer would normally be expected to engage.

Obtaining a sufficient understanding of its customers and the nature and purpose of the customer relationship, together with the ongoing analysis of actual customer behavior and the behavior of relevant peer groups, allows the LFI to develop a baseline of normal or expected activity for the customer, against which unusual or potentially suspicious transactions can be identified. TM compliance personnel should escalate for priority remediation any identified omissions or inaccuracies in relevant customer or beneficial ownership information or gaps or data quality issues in required transaction or payment message fields.

An effective TM program consists of the following core elements:

- **A well-calibrated risk-based framework:** The risks LFIs face are dynamic and the transactions they carry out may be varied and high in volume. LFIs should therefore review and enhance their TM frameworks regularly and upon the occurrence of specified "trigger events," such as material changes in the LFI's business or risk profile or its legal and regulatory environment, to ensure that

they remain tailored to the institution's financial crime risks. Incorporating feedback from the personnel handling the alerts to the TM system also helps in better calibration and tuning.

- **Robust training and risk awareness:** To ensure proper functioning and implementation of their TM programs, LFIs should ensure that personnel with TM responsibilities have adequate experience and expertise and receive role-specific training on the institution's TM policies, procedures, and risks.
- **Meaningful integration into the AML/CFT program:** LFIs should ensure that their TM systems and frameworks reinforce, and are reinforced by, the wider AML/CFT control environment of which they are a part. An effective TM program depends on the quality and completeness of data drawn from the LFI's customer and transactional systems and databases. In tandem, the outcomes of TM should inform the LFI's understanding and management of its financial crime risks, including by prompting off-cycle customer reviews and the application of enhanced scrutiny or additional controls to higher-risk customers or transactions.
- **Active oversight:** The LFIs' board and senior management should take an active role in overseeing the performance of their TM programs and the ongoing enhancement of TM systems on the basis of the institution's risks. Where the outcomes of TM are compromised by factors such as inappropriate calibration, process inefficiencies, staff issues, or system failures, it is necessary that the board (or a board-designated committee) and senior management be made aware of these issues in a timely manner so as to ensure that they are promptly and adequately remediated. The board and senior management should also communicate clear risk appetites within their institutions and set a strong tone from the top that the prevention, detection, and reporting of illegal or suspicious transactions are a priority. A quality assurance process should also play a crucial part in the TM program, by validating the review from accuracy and detail perspective. Any changes in the transaction codes or changes in the core banking system should be approved by senior management.

2.1. Risk Assessment

The design of an LFI's TM program should be informed by the LFI's risk assessment, so that TM 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, as well as the strength of the controls currently in place to mitigate these risks. The risk assessment serves a range of critical purposes, including but not limited to enabling an LFI to:

- understand the type of level of risk associated with its business relationships and transactions;
- develop risk-based policies, procedures and controls;
- make informed decisions with respect to resourcing and staffing;
- apply additional controls to areas of heightened risk; and
- ensure that the LFI's residual risks are within its risk appetite.

With respect to transaction monitoring specifically, the risk assessment can be used to ensure that each mode of transacting with or through the institution—domestically or internationally—is subject to a form of TM that is commensurate with its risks and is operating effectively to mitigate those risks. The risk assessment should be updated at periodic intervals (at least annually or otherwise as appropriate and justified by the required circumstances) and also upon the occurrence of "trigger events," such as material changes in the LFI's business or risk profile or the legal and regulatory environment.

2.2. Risk-Based Deployment of Transaction Monitoring Controls

TM can include manual monitoring processes and the use of automated and intelligence-led monitoring systems. In all cases, the appropriate type and degree of monitoring should appropriately match the ML/TF/PF risks of the institution's customers, products and services, delivery channels, and geographic exposure, and may therefore vary across an LFI's business lines or units, where applicable. TM programs should also be calibrated to the size, nature, and complexity of each institution. **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. LFIs utilizing automated systems should perform a typology assessment to design appropriate rule- or scenario-based automated monitoring capabilities and processes. While **smaller LFIs may rely on TM 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.

Examples of automated tools include 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 schedule), automated fraud detection systems, trade surveillance systems, and automated negative news screening tools. Examples of manual tools include unusual activity or unusual transaction reporting by business-line employees (including especially, but not limited to, customer relationship managers or those otherwise in customer-facing roles), reporting of potentially suspicious activity by LFI employees (including internal whistleblower reporting), manual reviews of document-based transactions (such as documentary trade finance transactions or loans), manual negative news screening, and periodic or event-based CDD reviews.

Particularly where purely manual processes are employed, LFIs should implement appropriate training on TM policies and procedures to ensure that personnel adhere to the internal processes for identification and referral of potentially suspicious activity. LFIs should be aware of all methods of identification and should ensure that their suspicious activity monitoring program includes processes to facilitate the transfer of internal referrals to appropriate personnel for further research. Regardless of whether automated or manual processes (or a combination of the two) are used to perform TM, it is the LFI's responsibility to demonstrate that the monitoring program is effective and appropriately risk based.

Where practicable and on a risk basis, LFIs should monitor transactions at the customer or relationship level, including across financial groups, and not only on an individual account basis, so as to obtain a complete view of a customer's transaction profile at the institution. Holistic monitoring of customers with multiple accounts is especially important for customers assessed to be politically exposed persons or as belonging to other high-risk categories.

2.3. Data Identification and Management

LFIs should have in place adequate processes to ensure that customer and transactional data feeding into their TM program (whether using manual or automated processes, or both) meets established data quality standards, that data is subject to testing and validation at risk-based intervals, and that identified data quality and completeness issues are remediated in a timely manner.

As an initial matter, LFIs should identify and document all data sources that serve as inputs into their TM program. TM data sources may include both internal customer databases, core banking or other transaction processing systems, and applicable "flat-file" databases, as well as external sources such as Society for Worldwide Interbank Financial Telecommunication ("SWIFT") message data. Source system documentation should include the identification of a system owner or primary party responsible for overseeing the quality of source data and addressing identified data issues. Where automated TM systems are used, LFIs should institute data extraction and loading processes to ensure a complete, accurate, and fully traceable transfer of data from its source to TM systems. LFIs should also ensure that staff's access rights to both source systems and TM systems are commensurate with their roles and responsibilities, so as to ensure that relevant staff can perform their duties effectively and that access is not extended to unauthorized persons or those no longer requiring system access.

Both prior to the initial deployment of a TM system or process and at risk-based intervals thereafter, LFIs should test and validate the integrity, accuracy, and quality of data to ensure that accurate and complete data is flowing into their TM program. 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 mandated and documented in the LFI's policies and procedures. Such testing can include data integrity checks to ensure that data is being completely and accurately captured in source systems and transmitted to TM systems, as well as the reconciliation of transaction codes across core banking and TM systems. Testing may also utilize quantitative data quality standards or benchmarks to track data quality over time and specify a threshold or range beyond which data irregularities or other data quality issues shall require corrective action.

In addition, LFIs 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 and ensure that any such irregularities caused by data integrity or other data quality issues are appropriately diagnosed and remediated. Where appropriate, a root cause analysis should be performed, and any findings and recommended remedial actions should be escalated to senior management to address the underlying issue in a timely manner.

2.4. Rule Definition and Pre-Implementation Testing

LFIs 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, as warranted. 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 diverges from expected or historical transactional activity or may otherwise be indicative of illicit activity, including the evasion of reporting or recordkeeping requirements.

TM rules may be automated or manual and should employ value and other thresholds and parameters that take into account the specific risks and contexts of the institution, as identified in the financial crimes risk assessment, and the specific product or service and customer type involved in the transaction. To this end, 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 the use of statistical tools or methods such as above-the-line and below-the-line testing, which involves increasing and decreasing the predetermined 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.

In order to identify patterns of potentially suspicious or illegal activity spanning multiple transactions, LFIs should group individual TM parameters and thresholds into multi-factor risk scenarios in order to more precisely target transaction patterns and behaviors consistent with known illicit financing typologies. Key typologies and associated indicators of relevance in the context of the UAE published by the FIU are included in the CBUAE's *Guidance for LFIs on Suspicious Transaction Reporting*.[4] 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. However, 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. In all cases, LFIs should maintain documentation that articulates the institution's current detection scenarios and their underlying assumptions, parameters, and thresholds.

Where automated systems are employed, LFIs should perform pre-implementation testing of TM rules and systems, using historical transaction data as appropriate. Such testing should include system integration testing to ensure compatibility of the TM system with source systems and other AML/CFT 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 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 system.

2.5. 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. In such a scenario, non-high scoring alerts could then be allocated to the staff using a "round robin" or any other technique in order to ensure a balanced and efficient distribution of alerts among staff. 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.

[4] Available at https://www.centralbank.ae/en/cbuae-amlcft.

2.6. Outcomes Analysis and Management Information Systems Reporting

LFIs should document and track TM outputs in order to identify and address any technical or operational issues and understand key risks or trends over time. Irregularities in TM system performance, including significant changes in the productivity of TM rules over time, may be indicative of underlying data quality or data integrity issues or of the need to recalibrate rule thresholds or parameters. 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) should be reported back to model owners for tuning and optimization. Where TM 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.

In addition, LFIs should ensure that senior management is regularly updated on the performance and output of their TM program, including through the provision of metrics, trends, and other MIS reporting generated by TM systems or produced by TM 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. TM-related 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 and that activity exceeding its risk appetite is addressed through appropriate risk mitigation measures, including but not limited to the use of account- or customer-based risk markers and/or activity, product, or service restrictions.

2.7. 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 systems and processes, including the continued relevancy of detection scenarios and assumptions and the calibration of rule threshold values and parameters. As with pre-implementation testing, post-implementation testing should include checks for system integration, data quality, and operational functionality, and should additionally include back-testing of TM rules to ensure that they remain current and effective in targeting riskier transactions and activity. Any proposed tuning or adjustment to TM rules, particularly material adjustments, should be subject to pre-implementation testing using sample or historical data to ensure the proper functioning of the new or revised rules, and should be reflected in updated TM documentation.

TM 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 TM 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 (as where model validation is performed by an internal audit department as part of independent testing of the AML/CFT program) or by the engagement of an external party not responsible

for model development or use. As a practical matter, some validation work may be most effectively done by model developers and users; it is essential, however, that such validation work be subject to critical review by an independent party, who should conduct additional activities to ensure proper validation. All model validation activities and identified issues should be clearly documented, and management should take prompt action to address model issues.

3. Sanctions Screening

As per Article 21.2 of Cabinet Decision 74, LFIs are required to perform regular searches against applicable sanctions lists of their customer databases, parties to any transactions, potential customers, beneficial owners, and persons and organizations with which the LFI has a direct or indirect relationship, as well as continuous searches of their customer database before conducting any transaction or entering into a business relationship with any person. Sanctions screening systems and processes are essential, but are also only as effective as the customer and transactional information used when comparing against applicable sanctions lists. Therefore, effectiveness depends critically on the completeness and accuracy of information obtained through the application of CDD/KYC measures and contained in payment instructions and other transactional data fields.

Sanctions compliance personnel should escalate for priority remediation identified omissions or inaccuracies in relevant customer or beneficial ownership information, as well as gaps or data quality issues in required transaction or payment message fields. On a risk basis, LFIs should perform sample testing of payment messages to ensure proper usage of message types and compliance with payment transparency requirements.

An effective sanctions screening program consists of the following core elements:

- **A well-calibrated risk-based framework:** The risks LFIs face are dynamic and the transactions they carry out may be varied and high in volume. LFIs should therefore review and enhance their sanctions screening frameworks regularly and upon the occurrence of specified “trigger events,” such as material changes in the LFI’s business or risk profile or its legal and regulatory environment, to ensure that they remain tailored to the institution’s financial crime risks.
- **Robust training and risk awareness:** To ensure proper functioning and implementation of their sanctions screening programs, LFIs should ensure that personnel with sanctions screening responsibilities have adequate experience and expertise and receive role-specific training on the institution’s sanctions screening policies, procedures, and risks.
- **Meaningful integration into the sanctions program:** LFIs should ensure that their sanctions screening systems and frameworks reinforce, and are reinforced by, the wider sanctions control environment of which they are a part. An effective sanctions screening program depends on the quality and completeness of data drawn from the LFI’s customer and transactional systems and databases. In tandem, the outcomes of sanctions screening should inform the LFI’s understanding and management of its financial crime risks, including by prompting off-cycle customer reviews and the application of enhanced scrutiny or additional controls to higher-risk customers or transactions, as warranted.

- **Active oversight:** The LFIs' board and senior management should take an active role in overseeing the performance of their sanctions screening programs and driving the ongoing enhancement of sanctions screening systems on the basis of the institution's risks. Where the outcomes of sanctions screening are compromised by factors such as inappropriate calibration, process inefficiencies, staff issues, or system failures, it is necessary that the board (or a board-designated committee) and senior management be made aware of these issues in a timely manner so as to ensure that they are promptly and adequately remediated. The board and senior management should also communicate clear risk appetites within their institutions and set a strong tone from the top that the implementation of targeted financial sanctions is a priority. A quality assurance process should also play a crucial part in the sanctions screening program, by validating the review from accuracy and detail perspective.

3.1. Risk Assessment

An LFI's risk assessment is a critical tool for ensuring that the institution has a complete, accurate, and up-to-date understanding of the sanctions risks to which their institution may be exposed, and for facilitating a risk-based approach to sanctions compliance. In the context of targeted financial sanctions, the risk-based approach cannot provide a justification for failing to apply sanctions-related controls, including sanctions screening, to *all* customer relationships and transactions, as defined below, which is a minimum legal requirement for all LFIs. Rather, the risk-based approach should be utilized by LFIs to apply additional or more rigorous controls—above the minimum legal requirement—to areas of heightened sanctions risk.

The LFI's risk assessment should include, at a minimum, an assessment of the customers, products and services, delivery channels, and geographies through which the LFI is most likely to engage, directly or indirectly, with sanctioned persons, parties, countries, or regions, as well as the strength of the controls currently in place to mitigate sanctions risks. The risk assessment should be updated at periodic intervals (at least annually or otherwise as appropriate and justified by the required circumstances) and also upon the occurrence of "trigger events," such as material changes in the LFI's business or risk profile or its legal and regulatory environment.

3.2. Risk-Based Deployment of Sanctions Screening Controls

Sanctions screening can include the manual review of customers and transactions against applicable sanctions lists, as well as the use of automated screening and interdiction software and systems. In all cases, the appropriate method of sanctions screening and the screening criteria employed should be appropriately calibrated to the sanctions risks presented by the institution's customers, products and services, delivery channels, and geographic exposure, and may therefore vary across an LFI's business lines or units, where applicable. Areas of heightened risk may require additional sanctions-related due diligence, more frequent or more intensive manual reviews of customers, counterparties, and their transactions, enhanced monitoring for transactions or behavior designed to evade sanctions controls, or the specialized training for sanctions compliance personnel in high-risk roles.

Sanctions screening controls should also be calibrated to the size, nature, and complexity of each institution. **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 sanctions screening systems that are less automated**, they should also still ensure that

these are appropriately executed to address the risks from their day-to-day transactional activity, as well as fully automated for the **update of any changes to the UN Consolidated List and the Local Terrorist List**.

Examples of automated tools include automated name screening tools that compare customer databases against applicable sanctions lists, live payment and other 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.

Examples of manual tools include manual reporting and escalations of potentially sanctions-related activity by LFI employees (including especially customer relationship managers and other business-line personnel), manual reviews of document-based transactions (such as documentary trade finance transactions or loans), and periodic or event-based CDD reviews.

Particularly where purely manual processes are employed, LFIs should implement appropriate training on sanctions screening policies and procedures to ensure that personnel adhere to the internal processes for identification and referral of potentially sanctions-related activity. LFIs should be aware of all methods of identification and should ensure that their sanctions screening program includes processes to facilitate the transfer of internal referrals to appropriate personnel for searches against applicable lists. Regardless of whether automated or manual processes (or a combination of the two) are used to perform sanctions screening, the onus is on the LFI to demonstrate that the screening program is effective and appropriately risk based.

3.3. Data Identification and Management

LFIs should have in place adequate processes to ensure that customer and transactional data feeding into their sanctions screening program (whether using manual or automated processes, or both) meets established data quality standards, that data is subject to testing and validation at risk-based intervals, and that identified data quality issues are remediated in a timely manner.

As an initial matter, LFIs should identify and document all data sources that serve as inputs into their sanctions screening program, including applicable customer databases and core banking or other transaction processing systems. Source system documentation should include the identification of a system owner or primary party responsible for overseeing the quality of source data and addressing identified data issues. Where automated sanctions screening systems are used, LFIs should institute data extraction and loading processes to ensure a complete and accurate transfer of data from its source to sanctions screening systems. LFIs should also ensure that staff's access rights to both source systems and sanctions screening systems are commensurate with their roles and responsibilities, so as to ensure that relevant staff can perform their duties effectively and that access is not extended to unauthorized persons or those no longer requiring system access.

Both prior to the initial deployment of a sanctions screening system or process and at risk-based intervals thereafter, LFIs should test and validate the integrity, accuracy, and quality of data to ensure that accurate and complete data is flowing into their sanctions screening program. 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 mandated and documented in the LFI's policies and procedures. Such testing can include data integrity checks to ensure that data is being completely and

accurately captured in source systems and transmitted to sanctions screening systems, as well as the reconciliation of transaction codes across core banking and sanctions screening systems. Testing may also utilize quantitative data quality standards or benchmarks to track data quality over time and specify a threshold or range beyond which data irregularities or other data quality issues shall require corrective action.

In addition, LFIs should put in place appropriate detection controls, such as the analysis of trends observable through MIS data and the generation of exception reports, to identify abnormally functioning sanctions screening logic and ensure that any such irregularities caused by data integrity or other data quality issues are appropriately diagnosed and remediated. Where appropriate, a root cause analysis should be performed, and any findings and recommended remedial actions should be escalated to appropriate senior management to address the underlying issue in a timely manner.

3.4. Screening Program Design and Pre-Implementation Testing

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". The concept 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 on a periodic basis and prior to entering into a customer relationship. 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".

Where automated systems are employed, LFIs should perform pre-implementation testing of sanctions screening systems, using historical transaction data as appropriate. Such testing should include system integration testing to ensure compatibility of the sanctions screening system with source systems and other 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 sanctions screening 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 sanctions screening system.

The following sections provide additional detail about system design and pre-implementation testing as these relate specifically to name screening and transaction screening processes respectively.

3.4.1. Name Screening

As per the Executive Office's *Guidance on TFS for Financial Institutions and Designated Non-financial Business and Professions*,[5] **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.** As indicated above, 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 on a periodic basis and prior to entering into a customer relationship.

[5] Available at: https://www.uaeiec.gov.ae/en-us/un-page#.

Data relevant for name screening may include:

- 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.

Not all data elements within an LFI's records are relevant for sanctions screening. When determining what reference data should be screened, an LFI should identify the data within its operations and records that is relevant to sanctions risk, determine how it is relevant, ensure it is conducive to effective screening, and differentiate it from data that is not relevant or suitable to screening. For example, the names of individuals and entities with whom the LFI has a relationship are relevant for screening against name-based sanctions lists but not for geographic (region- or country-based) sanctions programs. Likewise, while the data contained in the addresses of such individuals and entities may not be directly relevant for *screening* against name-based sanctions lists, this data may assist in differentiating a true name match from a false name match when *reviewing* apparent name screening hits.

An LFI should also define other data elements (such as date of birth, nationality, and place of birth) that may be relevant for sanctions screening in some situations but not others. Date of birth, for example, is relevant as a distinguishing factor to assess a potential or a true match from a false match on an individual and might be used for screening in combination with another attribute, such as a name. In each case, LFIs should weigh up the relative incremental value of screening the data element against the reliability of the data and whether an alert against the data will meaningfully assist in detecting or preventing a sanctions risk that would not be reasonably detected through other controls, or by screening different data attributes. The screening criteria used by LFIs to identify name variations and misspellings should be based on the level of sanctions risk associated with the particular product or type of transaction. For example, in a higher-risk area with a high volume of transactions, the LFI's interdiction software should be able to identify close name derivations for review.

An LFI's reference data is typically maintained in electronic files and is most effective when screened through an automated process and repeated at defined intervals. The use of manual screening can be considered when the risk is sufficiently low and where the reference data cannot be sourced reliably, either electronically or in a format necessary for automated screening. For example, if an LFI has identified only a small population of names requiring screening, it may choose to forego investing in an automated screening system and instead manually input these names into an online screening filter.

3.4.2. Transaction Screening

LFIs should screen all payments prior to completing the transaction (also referred to as "real-time" screening), utilizing all transaction records necessary to the movement of value between parties and at a

point in the transaction where detection of a sanctions risk is actionable to prevent a violation. The LFI should then identify which attributes within those records are relevant for sanctions screening and the context in which they become relevant. As with name screening, names of parties involved in a transaction are relevant for list-based sanctions programs, whereas addresses are more relevant to screening against geographic sanctions programs but can be used as identifying information to help distinguish a potential or true match from a false match under a list-based program. Other data elements, such as bank identification codes, may be relevant for both list-based and geographic sanctions programs.

Some data elements are more relevant for sanctions screening purposes when found in combination with other attributes or references. For example, detection of sectoral sanctions risk typically requires detection of multiple factors, such as those where both the targeted parties and the prohibited activities are involved. Where automated controls alone may not be capable of detecting both factors simultaneously, manual review of the associated activity may be required alongside review to confirm a true match to applicable sanctions lists. In addition, certain data elements offer little or no risk mitigation through screening, for example, amounts, dates, and transaction reference numbers have no relevance from a screening perspective, although they may be relevant for TM or other risk management purposes.

Data relevant for transaction screening 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, including any:
    - Importers and exporters, manufacturers, drawees, drawers, notify parties, and signatories;
    - Shipping companies, vessel names and International Maritime Organization (IMO) numbers, names of parties associated with the vessel (including ship owners, charterers, and captains), and freight forwarders;
    - Facilitators, such as insurance companies, agents, and brokers; and
    - Financial institutions, including issuing, advising, confirming, negotiating, claiming, collecting, reimbursing, and guarantor banks.
- Geographic details, including:
    - Addresses, countries, cities, towns, regions, ports, and airports (e.g., as contained within SWIFT Fields 50 and 59 or acquired through vessel tracking inquiries);
    - Phone or fax numbers and web addresses, insofar as these contain geographic or other relevant details;
    - Place of taking in charge, receipt, dispatch, delivery, or final destination;

- Country of origin, destination, and transshipment of goods or services; and
- Airport of departure or destination.

Transaction screening should be performed at a point in time where a transaction can be stopped and before a potential violation occurs. This typically occurs at a number of points in the lifecycle of a transaction, but certainly prior to executing any commitment to move funds. 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.

Transactional records are typically found in large volumes and within business processes predicated on speed of execution. These transaction types are generally in electronic form and conducive to systemic, automated screening. Some transaction types, however, still rely on documentation in various formats and varying methods of presentation. LFIs may employ text analytics tools such as optical character recognition ("OCR") that automatically convert paper documentation into electronic data that can then be screened against applicable sanctions lists, but some paper-based transactions, such as documentary trade finance transactions, may require manual screening processes, where relevant information is physically added into a system for screening. OCR requires quality assurance validation to ensure the information has been captured fully and accurately. Certain paper-based transactions, such as paper cheque clearing, where the volumes can be high and the manual screening process creates high rates of errors, may rely on controls other than screening, such as CDD/KYC processes, where the sanctions risks for the product are assessed as being low.

3.5. 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). LFIs' sanctions screening processes should also include searches for entities that are not themselves listed but that are owned or controlled mainly or fully by a listed person (also referred to as "shadow listed persons"). LFIs cannot conduct transactions with shadow listed persons and must freeze any funds or assets of a shadow listed person that they may hold as per Article 15 of Cabinet Decision 74. Although shadow designated persons, by their very nature, 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, such as adverse media reporting. LFIs should include such a list, together with any other internal lists (such as lists of customers exited for financial crime concerns) in its sanctions screening systems and processes.

Given the dynamic nature of targeted financial sanctions, LFIs should establish and implement sanctions list management procedures that enable the institution's sanctions screening program to adjust rapidly to changes published by sanctions authorities. The following considerations are relevant to effective list management, and each should be documented and reviewed on a regular basis, to ensure that the LFI's chosen approach remains in line with its risk appetite and in compliance with applicable legal requirements:

- **List selection:** The LFI should determine which sanctions lists are relevant for screening. Lists must include, at a minimum, all names on the UN Consolidated List and the Local Terrorist List, but may also include other jurisdictional lists as well as internal lists of persons known to have a sanctions nexus, lists of geographic terms (such as cities, regions, and ports), banking terms (such as BICs), and lists of prohibited goods or prohibited securities, where applicable. Although lists

issues by the UNSC or by the UAE Cabinet must be employed in the screening of all customers and transactions, as outlined above, other lists may be employed on a risk basis. For example, screening against lists of prohibited goods may be limited to the context of trade finance transactions, whereas such transactions likely would not need to be screened against sanctioned securities.

- **Sourcing of lists:** The LFI should determine which lists are to be generated internally and which lists are best sourced from external vendors, and the processes for generating and implementing such lists.
- **List maintenance:** The LFI should determine the processes for adding and removing lists or entries on internal lists, where screening is no longer required or where the result is within the institution's risk appetite. The LFI should identify and implement appropriate controls to ensure that lists remain up to date and that only appropriate individuals can add or remove lists or list entries.
- **Data enhancement:** The LFI should determine whether certain list entries should be modified or enhanced based on additional information.
- **Whitelisting:** The LFI may consider establishing and maintaining a "white list" of customer names or other data elements that have already been flagged and cleared through thorough due diligence by the LFI as false positives. These "white lists" may be used to improve the process related to screening by leveraging the results of past due diligence and reducing the number of false positives. While the LFI should not overly rely on such a list, and must diligently and continuously screen customers and transactions in case they are implicated in the updated UN Consolidated List and Local Terrorist List, the use of such a "white list" may assist the LFI in expediting the dispositioning in case of repeated false positive matches. LFIs should have documented procedures to managing and periodically reviewing and updating those "white lists" to account for the possibility that persons on a whitelist may later become sanctioned persons. Where automated screening tools are employed, the LFI should determine the management of rules for automatically eliminating potential hits caused by the interaction of certain list terms and frequently encountered data. Where manual screening processes are employed, the LFI should establish a process for manually reviewing potential hits against the whitelist.
- **Geographic scope of application:** Where the LFI has operations in multiple jurisdictions, the LFI should determine which lists should be screened in all jurisdictions of an LFI's operations and which, if any, could be screened only within a certain jurisdiction or several jurisdictions.
- **Exact matching versus "fuzzy logic":** The LFI should determine which lists should be deployed within the screening filter on an exact match basis, and which should use fuzzy matching (i.e., an algorithm-based technique to match one name or other string of words where the content of the information being screened is not identical—but its spelling, pattern, or sound is a close match—to the contents on a list used for screening).
- **Frequency of screening:** The LFI should determine the frequency or the triggers for static data screening, so as to account for additions to lists and changes in customer data.

List management procedures should be documented and subject to periodic review to ensure that list management practices remain aligned to the LFI's risk profile and risk appetite.

3.6. Outcomes Analysis and Management Information Systems Reporting

LFIs should document and track sanctions screening outputs in order to identify and address any technical or operational issues and understand key risks or trends over time. Irregularities in sanctions screening system performance, including significant changes in 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 sanctions screening search logic. Identified data quality or integrity issues should be reported back to designated data owners, and apparent screening logic issues should be reported back to model owners for tuning and optimization.

In addition, LFIs should ensure that senior management is regularly updated on the performance and output of their sanctions screening program, including through the provision of metrics, trends, and other MIS reporting generated by sanctions screening systems or produced by sanctions screening alert review and investigation teams. Such reporting may include an analysis of the number and type of screening hits and the proportion of apparent matches that are cleared as false positives compared to those that are confirmed as potential or true matches. Sanctions screening-related 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 and that activity exceeding its risk appetite is addressed through appropriate risk mitigation measures, up to and including account activity restrictions and customer exit.

3.7. 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 sanctions screening systems and processes, including threshold settings, screening rules, and the accuracy and completeness of data used in the screening process. Any proposed material adjustments to sanctions screening search logic should be subject to pre-implementation testing using sample or historical data to ensure the proper functioning of the new or revised logic, and reflected in updated sanctions screening documentation.

Sanctions screening 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 sanctions screening 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 (as where model validation is performed by an internal audit department as part of independent testing of the sanctions compliance program) or by the engagement of an external party not responsible for model development or use. As a practical matter, some validation work may be most effectively done by model developers and users; it is essential, however, that such validation work be subject to critical review by an independent party, who should conduct additional activities to ensure proper validation. All model validation activities and identified issues should be clearly documented, and management should take prompt action to address model issues.

4. Program Governance and Oversight

The following sections outline program governance expectations relating to TM and sanctions screening systems and processes.

4.1. Oversight, Management Reporting, and Auditing

The LFI's board of directors and senior management should exercise active oversight of the institution's key financial crimes risks and the controls in place to mitigate those risks. The board (or a board-designated committee) and senior management should receive regular reports on the institution's key risks and trends and the overall performance of AML/CFT and sanctions controls, and should review the institution's financial crimes risk assessment, any AML/CFT and sanctions audit and regulatory reports, and the institution's written AML/CFT and sanctions program. The AML/CFT and sanctions program should be subject to senior management approval, and the board and senior management should ensure that clear, current, and appropriate policies and procedures are put in place and that there are effective TM and sanctions screening systems supported by adequate internal expertise and resources.

TM and sanctions screening functions should be given clear and distinct responsibilities for their respective tasks in the TM and sanctions screening process chain (e.g., for alert handling and the filing of STRs/SARs). Additionally, as detailed above, LFIs are expected to implement effective reporting systems, to include quantitative MIS report as well as qualitative analysis of key risks and trends as appropriate, 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 sanctions screening 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. The LFI's independent testing function (whether internal or external) should ensure adequate TM and sanctions screening coverage of the LFI's customers, products, services, delivery channels, and geographies and may perform model testing and validation, as detailed above, as part of its AML/CFT and sanctions independent testing plan and methodology; otherwise, model testing and validation should be performed at periodic, risk-based intervals by a qualified and independent third party.

4.2. Use of Vendors and Other Third Parties

LFIs may use externally provided TM or sanctions screening services and other third-party providers to fulfil their legal and regulatory obligations to monitor and screen their customers and transactions. However, LFIs 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 sanctions screening processes will be centralized across business lines within the LFI, 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, LFIs 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. Vendors should provide appropriate testing results that show their product works as expected. They should also clearly indicate the model's limitations and assumptions and where the product's use may be problematic. LFIs should expect vendors to conduct ongoing performance monitoring and outcomes analysis, with disclosure to their clients, and to make appropriate modifications and updates over time.

LFIs are expected to validate their own use of vendor products. External models may not allow full access to computer coding and implementation details, so the LFI may have to rely more on sensitivity analysis and benchmarking. 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. If vendors provide input data or assumptions, or use them to build models, their relevance for the LFI's situation should be assessed. LFIs should obtain information regarding the data used to develop the model and assess the extent to which that data is representative of the LFI's situation. The LFI also should conduct ongoing monitoring and outcomes analysis of vendor model performance using the LFI's own outcomes. Systematic procedures for validation help the LFI to understand the vendor product and its capabilities, applicability, and limitations. Such detailed knowledge is necessary for basic controls of an LFI's operations. 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. LFIs should have contingency plans for instances when the vendor model is no longer available or cannot be supported by the vendor.

4.3. Role-Specific Training

LFIs should ensure that personnel responsible for performing TM and sanctions screening roles receive training that covers key financial crimes risks faced by the institution (such as common ML/TF/PF or sanctions evasion typologies), complex and higher-risk customer and transaction types relevant to TM and sanctions screening 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 sanctions screening systems or other technology relevant to the individual's role.

An LFI's TM and sanctions screening training should be based on an assessment of the institution's training needs, incorporated into wider AML/CFT and sanctions training plans and programs, and 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.

4.4. Record Keeping

According to Article 16 of the AML-CFT Law and Article 24 of the AML-CFT Decision, LFIs must maintain detailed records associated with their ML/FT risk assessment and mitigation measures as well as records, documents, data and statistics for all financial transactions, all records obtained through CDD measures for both the originators and the beneficiaries, account files and business correspondence, copies of personal identification documents, including STRs/SARs and results of any analysis performed. LFIs must maintain the records in an organized manner so as to permit data analysis and the tracking of financial transactions.

Records should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity. LFIs must make the records available to the competent authorities immediately upon request.

The statutory retention period for all records is at least five (5) years, from the date of completion of the transaction or termination of the business relationship with the customer, or from the date of completion of the inspection by the CBUAE, or from the date of issuance of a final judgment of the competent judicial authorities, or liquidation, dissolution, or other form of termination of a legal person or arrangement, all depending on the circumstances.

Annex 1. Synopsis of the Guidance

Purpose of this Guidance	Purpose	The purpose of this Guide is to assist the understanding and effective performance by CBUAE licensed financial institutions (LFIs) of their statutory obligations under the legal and regulatory framework in force in the UAE relating to the design, implementation, and maintenance of effective transaction monitoring and sanctions screening programs.
	Applicability	This Guidance applies to all natural and legal persons, which are licensed and/or supervised by the CBUAE, in the following categories: national banks, branches of foreign banks, exchange houses, finance companies and other LFIs as well as insurance companies.
Transaction Monitoring	Risk Assessment	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, as well as the strength of the controls currently in place to mitigate these risks. The risk assessment should be updated at periodic intervals (at least annually or otherwise as appropriate and justified by the required circumstances) and also upon the occurrence of "trigger events" such as material changes in the LFI's business or risk profile or the legal and regulatory environment.
	Risk-Based Deployment of TM Controls	In all cases, the type and degree of monitoring should appropriately match the ML/TF/PF risks of the institution's customers, products and services, delivery channels, and geographic exposure, and may therefore vary across an LFI's business lines or units, where applicable. TM programs should also be calibrated to the size, nature, and complexity of each institution. Where practicable and on a risk basis, LFIs should monitor transactions at the customer or relationship level, including across financial groups, and not only on an individual account basis, so as to obtain a complete view of a customer's transaction profile.
	Data Identification and Management	LFIs should identify and document all data sources that serve as inputs into their TM program. LFIs should test and validate the integrity, accuracy, and quality of data to ensure that accurate and complete data is flowing into their TM program. In addition, LFIs should put in place appropriate detection controls, such as the analysis of trends through management information systems (MIS) data and the generation of exception reports, to identify abnormally functioning TM rules or scenarios and ensure they are appropriately diagnosed and remediated.
	Rule Definition and Pre-Implementation Testing	LFIs should employ TM detection rules or scenarios that are designed to identify potentially suspicious or illegal transactions and elevate them for further review and investigation, as warranted. To this end, LFIs should: • Perform a typology assessment to design appropriate rule- or scenario-based automated monitoring capabilities and processes; • Perform risk-based customer and product segmentation, so that rule parameters and thresholds are appropriately calibrated; • Consider employ statistical tools or methods such as above-the-line and below-the-line testing, to better fine-tune their calibrations and reduce the volume of false-positive alerts; and • Perform pre-implementation testing of TM rules and systems to ensure compatibility of the TM system with source systems and other AML/CFT compliance infrastructure to ensure that it performs as anticipated in the operating environment.
	Alert Scoring and Prioritization	LFIs may consider assigning risk-weighted scores to TM alerts in order to prioritize higher-risk alerts for expedited review. 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.
	Outcomes Analysis and MIS Reporting	LFIs should document and track TM outputs in order to identify and address any technical or operational issues and understand key risks or trends over time. In addition, LFIs should ensure that senior management is regularly updated on the performance and output of their TM program, including through the provision of metrics, trends, and other MIS reporting.
	Post-Implementation Testing, Tuning, and Validation	On a periodic and event-driven basis, LFIs should reassess the functionality of TM systems and processes, including the continued relevancy of detection scenarios and assumptions and the calibration of rule threshold values and parameters. TM model testing and validation should be performed by individuals with sufficient expertise and appropriate level of independence from the model's development and implementation. All model validation activities and identified issues should be clearly documented, and management should take prompt action to address model issues.

Sanctions Screening	Risk Assessment	The LFI's risk assessment should include, at a minimum, an assessment of the customers, products and services, delivery channels, and geographies presenting the greatest sanctions risks, as well as the strength of the controls in place to mitigate these risks. The risk assessment should be updated at periodic intervals (at least annually or otherwise as appropriate and justified by the required circumstances) and also upon the occurrence of "trigger events," such as material changes in the LFI's business or risk profile or its legal and regulatory environment.
	Risk-Based Deployment of Sanctions Screening Controls	Sanctions screening programs should be appropriately calibrated to the sanctions risks presented by the institution's customers, products and services, delivery channels, and geographic exposure and may vary across an LFI's business lines or units, where applicable. Sanctions screening controls should also be calibrated to the size, nature, and complexity of each institution. LFIs should apply additional or more rigorous sanctions controls—such as enhanced customer or transactional due diligence, increased monitoring for sanctions evasion, and specialized training for personnel in high-risk roles—to areas of heightened sanctions risk.
	Data Identification and Management	LFIs should identify and document all data sources that serve as inputs into their sanctions screening program and test and validate the integrity, accuracy, and quality of data flowing into their sanctions screening program. In addition, LFIs should put in place appropriate detection controls, such as MIS trends analysis and exception reports, to identify abnormally functioning screening logic to ensure such irregularities are appropriately diagnosed and remediated.
	Screening Program Design and Pre-Implementation Testing	LFIs should perform pre-implementation testing of screening systems to ensure compatibility with source systems and other sanctions compliance infrastructure to ensure it performs as anticipated in the operating environment. 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. LFIs should screen all payments prior to completing the transaction (also referred to as "real-time" screening), utilizing all transaction records necessary to the movement of value between parties. Transaction screening should be performed at a point in time where a transaction can be stopped and before a potential violation occurs.
	List Management	LFIs should establish and implement sanctions list management procedures that enable the institution's sanctions screening program to adjust rapidly to changes published by sanctions authorities. List management procedures should be documented and subject to periodic review to ensure that list management practices remain aligned to the LFI's risk profile and risk appetite.
	Outcomes Analysis and MIS Reporting	LFIs should document and track screening outputs in order to identify and address any technical or operational issues and understand key risks or trends over time. In addition, LFIs should ensure that senior management is regularly updated on the performance and output of their screening program, including through the provision of metrics, trends, and other MIS reporting.
	Post-Implementation Testing, Tuning, and Validation	On a periodic and event-driven basis, LFIs should reassess the functionality of sanctions screening systems and processes, including threshold settings, screening rules, and the accuracy and completeness of data used in the screening process. Sanctions screening model testing and validation should be performed by individuals with sufficient expertise and level of independence. All model validation activities and identified issues should be clearly documented, and management should take prompt action to address model issues.
Program Governance and Oversight	Oversight, Management Reporting, and Auditing	LFIs' board (or board-designated committee) and senior management should receive regular reports on the key risks and trends and overall performance of the AML/CFT and sanctions controls. TM and sanctions screening functions should be given clear and distinct responsibilities for their tasks. TM and sanctions screening programs should be subject to independent testing by internal or external auditors.
	Use of Vendors and Other Third Parties	LFIs may use externally provided TM or sanctions screening services. However, LFIs are ultimately responsible for complying with AML/CFT and sanctions requirements. Systematic procedures for validation help the LFI to understand the vendor product and its capabilities, applicability, and limitations.
	Role-Specific Training	LFIs should ensure that TM and sanctions screening personnel receive role-specific training that covers key financial crimes risks, complex and higher-risk customer and transaction types, applicable legal and regulatory requirements, internal policies, procedures, and processes.