

# **Thematic Review of Screening Systems**

**In the UAE**

**Capital Markets Sector**

**2026**

## Contents

<b>1. Executive Summary .....</b>	<b>3</b>
<b>2. Background and Regulatory Context .....</b>	<b>4</b>
3. Scope and Coverage .....	5
4. Methodology and Testing Approach .....	6
4.1. Testing Design.....	6
4.2. Performance Measurement.....	6
<b>4.3. Benchmarking and Analysis .....</b>	<b>7</b>
<b>5. Key Findings.....</b>	<b>7</b>
5.1. Name Screening Systems .....	7
5.2. Transaction Screening Systems.....	7
5.3. System Efficiency and False Positives.....	8
5.4. Governance and Oversight.....	8
5.5. Data, Systems, and Technology .....	9
<b>6. Sectoral Insights and Development Trends.....</b>	<b>10</b>
7. Supervisory Expectations.....	11
8. Conclusion .....	12

## 1. Executive Summary

The Capital Market Authority (CMA) has conducted a thematic review of **name screening and transaction screening systems** across regulated financial institutions within the UAE capital market sector.

This review forms part of CMA's **risk-based supervisory framework** and supports the UAE's efforts to enhance the effectiveness of preventive measures in line with **Federal Decree-Law No. (10) of 2025** and its Executive Regulation, as well as international standards set by the Financial Action Task Force (FATF).

The assessment was performed using **independent and standardised testing methodologies**, enabling benchmarking of system performance under both baseline and practical operating conditions.

The results indicate that **screening systems are widely implemented across the sector and are embedded within institutions' financial crime control frameworks**. Institutions generally demonstrate awareness of their obligations regarding sanctions screening and targeted financial sanctions. At the same time, the review identified **variability in system performance and maturity across institutions**.

From an effectiveness perspective, while systems generally perform well in identifying clear matches, **performance varies under more complex matching scenarios (such as small spelling differences or alternative name forms)**, reflecting differences in system configuration, calibration practices, and matching capabilities.

From an efficiency perspective, elevated alert volumes were observed in several cases, indicating opportunities to optimise system parameters and alert management processes. Institutions are encouraged to define clear internal performance metrics (e.g. alerts per match and false positive rates) to support objective monitoring, calibration, and effective oversight.

The review also highlighted **differences in governance, oversight, and the use of management information**, particularly in ongoing monitoring of system performance and in continuous improvement practices.

These observations are primarily linked to factors such as **different approaches to system tuning, reliance on external (vendor) solutions, and varying levels of internal technical understanding**, which influence how effectively screening systems operate in practice.

Overall, the thematic review reflects a sector with established core frameworks, with continued progress required to ensure **consistent performance, optimisation, and alignment with evolving risks and international expectations**.

CMA will continue to engage with regulated entities to support **targeted enhancements, strengthened governance, and ongoing system optimisation**, ensuring that screening systems operate effectively, risk-based, and sustainably over time.

## 2. Background and Regulatory Context

The UAE has established a comprehensive framework to combat money laundering, terrorist financing, and proliferation financing, including **Federal Decree-Law No. (10) of 2025** and its Executive Regulation, which require financial institutions to implement effective, risk-based controls and ongoing monitoring of financial crime risks.

Within this framework, **name screening and transaction screening systems** represent key preventive measures to identify sanctioned individuals, entities, and high-risk activities, and to ensure compliance with Targeted Financial Sanctions obligations.

In line with its supervisory mandate, the CMA conducted this thematic review as part of its **risk-based supervisory programme**, with the objective of assessing, on a sector-wide basis, how screening systems operate in practice.

The review aims to:

- Evaluate the **effectiveness of screening systems in identifying sanctioned parties**, including under practical operating conditions
- Assess the **efficiency of systems and alert management processes**
- Identify **variations in implementation and maturity across institutions**

- Support **continuous enhancement and alignment with international standards**, particularly FATF expectations

This thematic review also provides a basis for **sector-wide insights and supervisory engagement**, supporting the ongoing development of screening frameworks as a core component of financial crime risk management.

### 3. Scope and Coverage

The thematic review was conducted as a **market-wide horizontal assessment** across a representative sample of regulated financial institutions within the UAE capital markets sector.

The review covered **26 Licensed Financial Institutions (LFIs)** and assessed 46 screening systems, encompassing both name and transaction screening frameworks.

The review included:

- **Name screening systems**, applied at onboarding and on an ongoing basis for customers, beneficial owners, and related parties; and
- **Transaction screening systems**, applied to payment flows and transactional activities to identify potential sanctions exposure

A combination of **automated and manual screening processes** was assessed, reflecting differences in institutional size, business models, and risk profiles.

The scope focused primarily on screening against:

- **United Nations Security Council sanctions lists**, and
- **UAE local terrorism and sanctions lists**, in line with national obligations under Targeted Financial Sanctions frameworks

The review also considered the **end-to-end operation of screening controls**, including system configuration, calibration practices, alert handling processes, and governance arrangements.

This approach enabled **consistent benchmarking and comparative analysis**, while also identifying **variations in implementation and system maturity across institutions**.

## 4. Methodology and Testing Approach

The thematic review was conducted using a **structured, independent, and outcome-focused methodology** to assess the performance of screening systems in practice across participating institutions. To ensure consistency and comparability, the CMA applied **standardised testing methodologies across all 46 screening systems**, supported by independent testing.

### 4.1. Testing Design

The testing framework was designed to evaluate system performance under both baseline and practical operating conditions, using three types of datasets:

- **Control datasets (exact match)** to assess baseline detection capability
- **Variation-based datasets** to assess system performance under realistic conditions, including differences such as spelling variations, alternative name orders, and common Arabic–Latin transliteration variants
- **Clean datasets** to assess system efficiency and the level of non-relevant alerts generated

This approach enabled a balanced assessment of both **detection capability and operational efficiency**.

### 4.2. Performance Measurement

System performance was assessed using key indicators, including:

- **Detection capability** (the ability to identify true matches), measured based on the proportion of correctly identified matches across tested datasets
- **Alert volumes and quality**, assessing the level of non-relevant alerts generated, with alert quality referring to the proportion of alerts that represent true matches versus false positives
- **Consistency of outcomes** across different testing scenarios

These indicators were used to evaluate how effectively systems operate in line with their intended purpose.

### 4.3. Benchmarking and Analysis

Results were benchmarked across institutions to identify **sector-wide patterns, variations in system performance, and differing levels of implementation maturity.**

The analysis was complemented by a review of:

- **System configuration and calibration practices**
- **Governance and oversight arrangements**
- **Data inputs and list management processes**

This methodology provided a **holistic and comparable view of screening system performance**, supporting evidence-based supervisory insights and alignment with international practices

## 5. Key Findings

### 5.1. Name Screening Systems

The review indicates that **name screening systems are widely implemented and embedded within onboarding and ongoing monitoring processes** across institutions.

From an effectiveness perspective, systems generally demonstrate **strong capability in identifying clear and direct matches**. At the same time, **variability in performance was observed under more complex matching scenarios**, reflecting differences in system configuration, calibration practices, and matching logic across institutions.

These variations highlight the importance of **ongoing tuning and optimisation of screening parameters**, particularly to ensure consistent performance under practical operating conditions.

### 5.2. Transaction Screening Systems

Transaction screening controls are established across institutions and form an important layer of defence in identifying potential sanctions exposure within payment flows.

Systems generally demonstrate the ability to **identify transactions involving relevant risk indicators**, supported by defined alert generation and escalation processes.

Variations were observed in the **level of system sophistication and calibration approaches**, particularly in relation to scenario design, parameter settings, and the use of automated controls, reflecting differing levels of system maturity across institutions.

### 5.3. System Efficiency and False Positives

The review identified that institutions are actively managing screening alerts through established processes and control frameworks.

However, in a number of cases, **elevated alert volumes were observed**, particularly for non-relevant matches. This indicates opportunities to further optimise system calibration and filtering logic to enhance efficiency.

Effective alert management remains critical to ensure that **investigative resources are appropriately focused and that relevant alerts are identified and escalated in a timely manner**.

### 5.4. Governance and Oversight

Governance frameworks supporting screening systems are in place across institutions, with defined roles and responsibilities for compliance and risk management functions.

The review identified **differences in the level of senior management oversight and the use of management information**, particularly in relation to monitoring system performance and driving continuous improvement.

Strengthening governance practices, including **regular review of system performance and testing outcomes**, will further support effective implementation.

## 5.5. Data, Systems, and Technology

Screening systems across the sector are supported by a combination of **established vendor solutions and internally developed configurations**, reflecting a range of operational models and levels of technological sophistication.

Institutions generally demonstrate the use of **automated screening tools integrated within core systems**, supporting both customer-level and transaction-level screening processes.

At the same time, the review identified variations in data quality, system integration, and configuration practices, which can influence overall system performance. In particular:

- **Differences in data standardisation**, accuracy, and completeness may affect matching accuracy
- **Variability in system integration** across platforms may impact end-to-end screening effectiveness

**Divergence in configuration and parameter settings** further reflects differing levels of system optimisation. **For example**, even a well-configured system may fail to identify matches where key customer data (such as date of birth, nationality, or identification details) is incomplete or inconsistent.

These observations are not uncommon in evolving environments and highlight the importance of **ongoing data management, system alignment, and configuration refinement**.

However, the financial institutions are emphasising an increasing focus on:

- Enhancing **data quality and governance frameworks**
- Strengthening **integration between screening systems and core platforms**
- Leveraging **advanced technologies and automation capabilities**
- Improving internal understanding of **system logic, filters, and matching algorithms**

Overall, the regulated financial sector demonstrates having adopted a **solid technological foundation**, with continued progress required to ensure that systems operate in a fully integrated, data-driven, and risk-aligned manner.

## 6. Sectoral Insights and Development Trends

The thematic review provides a comprehensive view of how screening frameworks are evolving across the financial sector and highlights a number of **positive development trends**.

Institutions are increasingly moving towards a more **risk-based and data-driven approach** in the design and operation of screening systems, aligning with regulatory expectations and international standards.

**Key developments observed include:**

- **Increased adoption of independent testing and validation practices**, supporting a more structured and evidence-based approach to assessing system performance
- Growing focus on **system calibration and optimization**, particularly to enhance both detection capability and operational efficiency
- Enhanced attention to **governance and oversight**, including more active involvement of senior management and improved use of management information
- Progressive improvements in **data quality and system integration**, supporting more consistent and reliable screening outcomes
- Greater internal understanding of **system configuration, matching logic, and parameter setting**, reducing reliance on external solutions over time.

These developments indicate a clear shift from viewing screening systems as **static compliance tools** to recognising them as **dynamic risk management controls** requiring continuous monitoring and refinement.

Overall, the regulated financial sector demonstrates a **positive trajectory of development**, with institutions proactively enhancing their frameworks to ensure alignment with evolving risks, regulatory expectations, and international best practices.

## 7. Supervisory Expectations

Based on the outcomes of the thematic review, the CMA expects all regulated entities to ensure that their screening frameworks operate effectively, are risk-based, and are **subject to continuous enhancement**.

Institutions are expected to ensure that screening systems are **appropriately calibrated and capable of identifying relevant matches under practical operating conditions**, while maintaining a balanced approach to alert generation and operational efficiency.

**In this context, the regulated financial institutions should:**

- Maintain **well-calibrated and properly tuned systems**, aligned with their risk profile, to support consistent detection outcomes.
- Be reminded that they remain fully **accountable for the effectiveness of screening systems**, and reliance on third-party vendors does not mitigate this responsibility.
- Implement measures to **optimise alert volumes**, ensuring that non-relevant alerts are managed without impacting detection capability.
- Conduct **regular risk-based testing and validation**, including following system changes or where performance considerations arise.
- Ensure that testing is **independent, evidence-based and appropriately documented**.
- Strengthen **governance and oversight frameworks**, with clear accountability and active senior management involvement.
- **Strengthen governance practices**, including regular (e.g. on a quarterly basis) reviews of system performance and testing outcomes at an appropriate senior management or committee level, with clear ownership and accountability, will further support effective implementation.
- Establish and utilize **relevant management information**, including performance metrics such as alert volumes, outcomes, and testing results
- Maintain **timely and accurate sanctions list updates**, supported by strong data quality and integrity controls.

- Ensure that systems are **appropriately configured, integrated, and maintained**, in line with operational and risk requirements.
- Provide **adequate training and capability development** for staff involved in screening and alert handling.
- Conduct **internal reviews and gap analyses**, and implement timely enhancement measures with appropriate supporting documentation.

The CMA will continue to engage with regulated entities to monitor progress and may request **evidence of system performance, testing outcomes, and remediation actions** as part of ongoing supervisory activities.

## 8. Conclusion

The thematic review confirms that **screening frameworks are established across the sector and form a key component of financial crime risk management within regulated financial institutions.**

The review also highlights that, while core controls are in place, **continued enhancement is required to ensure consistent performance, optimisation, and alignment with evolving risks and international expectations.**

Strengthening the effectiveness and efficiency of screening systems remains critical to mitigating risks related to **sanctions evasion, terrorist financing, and proliferation financing**, and to supporting the integrity and resilience of the UAE financial system.

The CMA will continue to adopt a **risk-based and outcomes-focused supervisory approach**, engaging with regulated entities to support ongoing improvements and ensure that **screening systems operate effectively, proportionately, and sustainably over time.**