AML · 26 JULY 2026 · 11 MIN READ

UAE AML Compliance in 2026: A Board-Level Operating Framework for DNFBPs

The UAE's updated AML framework expects risk ownership, independent compliance judgment and evidence that controls work in practice—not a policy file that is opened only before an inspection.

Akash Chetwani, CFA
SENIOR PARTNER · ADVISORY

IRAA Global Advisory

EDITORIAL GUIDE

Contents

AML · 11 MINUTE READ · JULY 2026

The UAE's updated AML framework expects risk ownership, independent compliance judgment and evidence that controls work in practice—not a policy file that is opened only before an inspection.

> The UAE’s anti-money laundering framework changed materially in late 2025. For Designated Non-Financial Businesses and Professions, the practical message is clear: compliance must be directed, resourced and tested as a management system, not treated as a file maintained by one employee.

Federal Decree-Law No. 10 of 2025 and Cabinet Resolution No. 134 of 2025 form the current federal AML, counter-terrorist-financing and proliferation-financing framework. The Executive Regulations became effective on 14 December 2025. They expressly connect senior management with strategic decisions affecting risk management, compliance policies and operational governance.

Key facts for business leaders

WHO IS IN SCOPE?	DNFBPs include real-estate brokers and agents, dealers in precious metals and stones above the applicable cash threshold, independent accountants and auditors, trust and company service providers, and other specified activities.
RISK ASSESSMENT	The business must identify, understand, manage, assess and document its crime risks in proportion to its nature and size.
REPORTING	Suspicion must be reported immediately and without delay through the Financial Intelligence Unit’s approved channel, regardless of transaction value.
RETENTION	Relevant transaction, due-diligence and monitoring records generally must be retained for at least five years, calculated from the applicable event and, in some cases, the latest relevant proceeding.

Start by confirming whether the business is a DNFBP

Many compliance failures begin with an incorrect scope decision. A general trading or consulting company is not automatically a DNFBP merely because it handles payments or employs an accountant. The analysis turns on the regulated activity performed for or on behalf of customers.

The 2025 Executive Regulations identify, among others, real-estate brokers and agents concluding purchase or sale transactions for customers; dealers in valuable metals and precious stones carrying out linked or single cash transactions of at least AED 55,000; and specified professional service providers. The Ministry of Economy supervises relevant DNFBPs at state level and in commercial free zones, while other sectors may fall under another supervisory authority.

Management should document its scope conclusion, the licences and activities reviewed, the regulator responsible and the date of the analysis. A business entering a new service line, acquiring another entity or changing how it serves customers should revisit the conclusion before launch.

Make the enterprise risk assessment operational

The law requires more than assigning every customer a generic “low”, “medium” or “high” label. The enterprise risk assessment should consider customer characteristics, countries and geography, products and services, transactions and delivery channels. It should reflect the UAE National Risk Assessment and relevant sectoral guidance.

A useful assessment links each identified risk to a control, owner and evidence source. If complex legal structures are considered high risk, the control may require a complete ownership chart, reliable verification of natural-person beneficial owners, source-of-wealth evidence and senior approval. If cash is a material exposure, the assessment should address thresholds, linked transactions, third-party payments and reporting triggers.

The document should be updated on an ongoing basis. “Annual review” is not a substitute for event-driven change. A new jurisdiction, remote onboarding tool, virtual-asset payment option or outsourced customer-verification provider can change risk immediately. Article 24 of the Executive Regulations requires risk assessment before launching new products, practices or technologies.

> *“A risk assessment is credible only when it changes what the business does.”*

Design customer due diligence around decisions

Customer due diligence should establish who the customer is, who ultimately owns or controls it, the purpose and intended nature of the relationship, and whether activity remains consistent with that understanding. It is not completed merely by collecting a passport and trade licence.

For a corporate customer, the file should connect registration records, authorised signatories, ownership, beneficial ownership, business activity and expected transaction profile. For higher-risk cases, enhanced due diligence may include source of funds and wealth, additional independent evidence, the reasons for complex ownership, and senior-management approval. Foreign politically exposed persons require appropriate detection systems and senior approval before establishing or continuing the relationship.

Where adequate due diligence cannot be performed, the business is prohibited from establishing or continuing the relationship or executing the transaction, and must consider whether a suspicious transaction report is necessary. Teams therefore need a defined route for declining, pausing or exiting business without allowing commercial pressure to override the control.

Give the compliance officer real independence

The Executive Regulations require appointment of a compliance officer at management level who has independent decision-making authority, competence and experience. The role includes monitoring crime-related transactions; examining internal alerts; deciding whether to report or retain a matter with reasons; reviewing systems and procedures; and reporting directly to senior management.

Independence is undermined if the same person must obtain sales approval to raise an alert, cannot access customer or transaction data, or is rewarded solely for commercial conversion. The board or owners should approve the appointment, mandate, access rights, resources and escalation route. Deputies and continuity arrangements are also important during leave or turnover.

Periodic reports should be decision-oriented. Useful metrics include overdue reviews, high-risk customers, screening alerts, unusual-activity cases, reports filed, training completion, quality testing, regulator requests and remediation progress. A “zero reports” metric is not automatically positive; it may indicate a weak detection process.

Build a defensible suspicious-activity process

DNFBPs must maintain indicators that identify suspicion and update them as criminal methods evolve. When there is suspicion or reasonable ground to suspect that a transaction, attempted transaction or funds relate to a crime, the business must notify the FIU immediately and without delay through the approved electronic system or other approved means. The obligation applies regardless of value.

The internal workflow should preserve confidentiality. Directors, officers and employees are prohibited from disclosing to the customer or another person that a report has been or may be submitted, or that an investigation is underway. Frontline teams need scripts and escalation guidance so that routine questions do not become tipping-off.

An alert that is not reported should still have a clear, dated rationale supported by the information reviewed. An alert that is reported should retain the submitted report, supporting documents and follow-up communication, with access restricted to authorised personnel.

Retain records that reconstruct the transaction

The current regulations generally require transaction and commercial records for at least five years from completion of the transaction or termination of the relationship. Due-diligence, monitoring, correspondence, identification, analysis and reporting records are also subject to at least five years, with the period calculated by reference to the latest of specified events such as an inspection, investigation or final judgment.

Records must be organised so that an individual transaction can be reconstructed, data can be analysed and financial flows traced. Scattered inboxes and unlabelled scans rarely meet that standard. A retention schedule should cover the core system, archived documents, chat-based instructions, screening evidence, approval logs and outsourced-provider records.

A 90-day board implementation agenda

01	**Confirm scope:** Map licensed activities to the 2025 DNFBP definitions and identify the correct supervisor.
02	**Refresh risk:** Update the enterprise assessment for customers, geography, services, channels and new technology.
03	**Strengthen authority:** Approve the compliance officer’s mandate, independence, data access, budget and deputy.

04	**Test files:** Sample customer files from onboarding through monitoring, approval, screening and closure.
05	**Test alerts:** Walk through an STR, a sanctions match and a no-report decision without using live customer data.
06	**Track remediation:** Give every gap an accountable owner, target date and evidence of closure.

The strongest AML programme is visible in everyday choices: which customers are accepted, what evidence is required, how exceptions are approved and how quickly unusual activity reaches an independent decision-maker. When senior management treats those choices as part of business quality, compliance becomes more reliable and commercial decisions become easier to defend.

Official sources

1. **Federal Decree-Law No. 10 of 2025 on AML, CFT and Proliferation Financing**
2. **Cabinet Resolution No. 134 of 2025: Executive Regulations**
3. **Ministry of Economy: AML/CFT resources for DNFBPs**

Online edition: **https://iraaglobal.com/insights/uae-aml-compliance-2026-board-framework-dnfbps/**

ABOUT THE CONTRIBUTOR

Akash Chetwani, CFA

SENIOR PARTNER · ADVISORY

Cross-border advisory for professionals, founders, investors, and globally connected families.

PHONE	+971 56 921 0222
EMAIL	info@iraaglobal.com
PROFILES	**LinkedIn** · **Contributor page and articles**

IRAA GLOBAL
AUDIT · TAX · ADVISORY

A connected advisory firm for businesses operating across borders.

OUR EXPERTISE

Audit & Assurance	Corporate Tax & VAT
Accounting & Bookkeeping	Finance & CFO Advisory
AML, Risk & Compliance	Business Advisory & Setup
Human Resources Advisory	AI, Technology & Digital Assets
India-UAE Cross-Border Advisory	Private & Family Advisory

IRAA GLOBAL

AUDIT · TAX · ADVISORY

Insight beyond numbers.

IRAA Global Advisory

503 Mustafawi Carpet Building, Sharaf DG Metro Exit 1

Dubai, United Arab Emirates

+971 56 921 0222 · +971 50 677 9455

info@iraaglobal.com · www.iraaglobal.com

LAYOUT & DESIGN BY SURESH TAMANG