

AML/CFT GOVERNANCE FRAMEWORK FOR DNFBPs

➤ Essential pillars of an effective AML/CFT governance framework

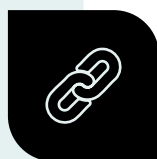
An effective Anti-Money Laundering/Combating Financing Terrorism (AML/CFT) governance framework is essential for deterring and detecting financial crime.

The pillars of an AML/CFT governance framework described in this Quick Guide are aligned with the applicable AML regulations in the UAE, as well as international standards, such as those established by the Financial Action Task Force (FATF).

Effective AML/CFT governance framework



Governance



Systems & controls



Training



Record keeping & reporting



Assurance & independent testing



Governance



Roles & Responsibilities

Establish clear roles and responsibilities within your firm and ensure appropriate oversight of staff engaging in activities that pose money laundering and terrorism financing (ML/TF) risks.



Training

Develop adequate training programs for your staff.

Ensure periodic and up-to-date staff training, at least annually. Your customer-facing staff may need additional trainings as opposed to non-customer facing staff. Maintain training logs of trainings conducted.



Senior Management Updates

Regularly update your board of directors, leadership and senior management on compliance initiatives, deficiencies identified, suspicious transactions reported, and actions taken.



Testing

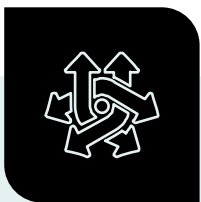
Develop, implement, and maintain independent quality assurance testing programs to evaluate the effectiveness of the controls in place.



Reporting

Develop and maintain a reporting system that accurately and timely captures information on the ongoing status of your AML/CFT program. This includes, but is not limited to, maintaining a log for the number of customers rejected and terminated relationships, transactions monitored, alerts generated, and suspicious transactions reported. Additionally, you must maintain adequate systems and processes for reporting of STRs/SARs via the goAML system.

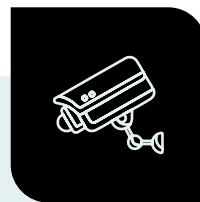
➤ Systems and Controls



Systems*

Implementing adequate systems in your firm is a key component to an effective AML/CFT governance framework. These include:

- Complying with Federal AML Legislation, Rules and Regulations applicable to your firm
- Conducting ongoing sanctions screening on your clients
- Identifying adverse media that may arise after onboarding your customer
- Identifying suspicious activities that are not aligned with your customer's profile
- Enabling your firm to provide an appropriate audit trail of a specific transaction



Controls

Effective controls ensure that the AML/CFT program is functioning as intended. The controls must be approved by senior management, reviewed for effectiveness, and continuously updated. These include:

- Developing an adequate AML/CFT program
- Carrying out an adequate Business Risk Assessment (BRA)
- Developing an adequate Customer Risk Assessment (CRA)
- Developing adequate procedures for conducting Customer Due Diligence (CDD), including ongoing reviews
- Developing a procedure for customer and transaction monitoring
- Ensuring that record-keeping requirements are constantly met
- Ensuring that all employees comply with the relevant requirements of your firm's policies and procedures

(*) Note that it is the responsibility of the firm, senior management and MLRO to conduct an annual review of its systems in place

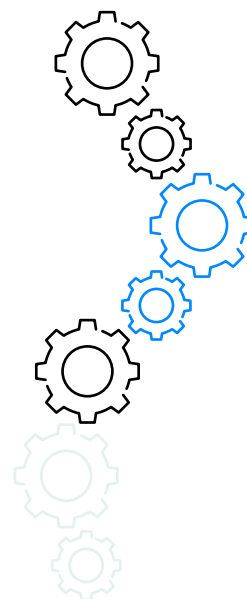
➤ Training



AML/CFT training for employees

Conduct initial and annual AML/CFT training to all relevant employees. The training must enable your employees to understand:

- the responsibilities of the MLRO and his deputy
- the fundamentals of relevant UAE AML/CFT laws and guidance
- the business' AML/CFT policies, procedures, systems and controls
- how to deal with transactions, risks and other activities that may relate to ML/TF
- the procedure in place for reporting internal suspicious activity and transaction reports to the MLRO
- the type of activities that may be a suspicious activity reportable to the MLRO
- the different types of typologies and trends applicable to your business
- the roles and responsibilities of the employees in combating money laundering (deleted and here)
- relevant findings, recommendations, guidance, directives, resolutions, Sanctions, notices or other requirements applicable to the firm



Good AML/CFT training is...



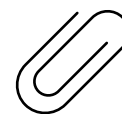
...tailored to the nature of your business, including products, services, customers, distribution channels, business partners and transactions complexity offered by your business

...inclusive of different levels of money laundering and terrorism financing risks and vulnerabilities associated with its business activities

...up-to-date with current AML/CFT rules and regulations, trends and techniques

➤ Record Keeping and Reporting

The retention period for AML records is at least 6 years, including KYC records from the date your business relationship with your customer ended, a transaction is completed or a Suspicious Transaction Report ("STR") or a regulatory notification is made (whichever occurs last). You are expected to be able to provide any requested records within one working day.



Transaction records

You must maintain operational and statistical records, documents and information concerning all transactions made or processed by your business. For example:



- Customer correspondence, requests and other forms related to transactions and related agreements
- Customer payment advices, receipts, invoices, and billing notifications
- Escrow or fiduciary account transaction records
- Sale, purchase, lease and other agreements
- Statistics and analytical data related to customers' financial transactions, such as their values, volumes, currencies and interest rates
- Records relating to justification of large or unusual transactions

CDD records

CDD records is the information and evidence that provides details of your customers. For example:



- Individual and corporate customer information (e.g. onboarding documentation, CDD and Enhanced CDD collected)
- Evidence of ongoing CDD and monitoring of business relationships
- CDD records must be kept for at least 6 years from the date the customer relationship ends

Training records

This includes maintaining records of AML/CFT trainings conducted for relevant employees, including the dates when the trainings were given, the nature of the training and the names of employees who received the training.



Reporting

Your firm has ongoing reporting obligations to your Board (or governance body) and the Regulator. These include, for example the annual AML Return, semi annual returns and STRs/SARs reporting.



You must ensure that you have adequate systems and controls in place to ensure on time reporting.

➤ Assurance and independent testing

An independent review must be conducted periodically on your firm's AML/CFT Framework to test the effectiveness and adequacy of your controls relating to combating money laundering and terrorism financing. The review can be conducted internally or by a third-party provider.

You must ensure that your independent audit function is appropriately staffed and has the required competencies and experience to effectively assess the adequacy of your AML/CFT framework.

Some smaller-sized DNFBPs may not have an internal audit unit. If you do not have an internal, independent audit function, you must engage a qualified third party to perform this function for you.



Audit scope must include the following components:

- Examining the adequacy of your AML/CFT and CDD policies, procedures and processes
- Assessing the adequacy of AML/CFT trainings
- Reviewing all the aspects of any AML/CFT compliance functions outsourced to third parties
- Reviewing your case management and transaction monitoring systems (e.g. handling of unusual transactions and referrals of unusual or suspicious activities from business lines)



Factors determining the frequency and extent of audit:

- Consideration of the National Risk Assessment* ("NRA") and other relevant risk assessments
- The nature, size, complexity and geographic scope of your business (including results of business risk assessments)
- Risk profile relating to products and services provided
- Internal and external developments in relation to money laundering and terrorism financing risks

(*) The Financial Action Task Force (FATF) defines NRA as a process whereby a country identifies, analyzes, and evaluates the ML/FT risks that it faces. This entails analyzing the economic sectors and activities that are most vulnerable to these risks, as well as the methods and channels that criminals use to launder money or finance terrorism.

You must take into account the results of the most recent NRA in the UAE, including the ML/FT vulnerabilities and risk typologies specific for your sector and type of DNFBP. The most recent results of NRA for the UAE are available at:

<https://www.moec.gov.ae/documents/20121/465917/UAE+Risk+Assessment+Outreach+Program+1.pdf>

