RapidAML

# Crafting Effective AML/CFT Policies: Best Practices for UAE DNFBPs and VASPs

www.rapidaml.com

info@rapidaml.com

It is important for Designated Non-Financial Businesses and Professions (DNFBPs)and Virtual Asset Service Providers (VASPs) to design their AML/CFT framework and implement AML/CFT policies and procedures to counter the risks of money laundering and terrorist financing. This article provides a detailed understanding of best practices for crafting effective AML/CFT policies and procedures.

# Table Of Content

# What is an **AML Policy**

AML policy is a formally drafted document approved by the senior management of an organisation.  The AML policy lays down the procedures, steps, and methodologies to be utilised by the organisation for combating the instances of money laundering (ML), financing terrorism (FT), and proliferation financing (PF) of weapons of mass destruction (WMD) to ensure compliance with the Federal Decree-Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and the Financing of Illegal Organisations in the UAE.

# Why do **DNFBPs and VASPs** need an AML/CFT Policy

**The Designated Non-Financial Businesses and Professions (DNFBPs) and Virtual Assets Service Providers (VASPs) operating in the UAE are required to ensure compliance with the UAE federal laws designed to combat ML, FT, and PF.**

The Cabinet Decision No. 10 of 2019 on the Implementing Regulation of Federal Decree-Law No. 20 of 2018 and Combating the Financing of Terrorism and Illegal Organisations and Guidelines for Designated Non-Financial Businesses and Professions require the DNFBPs and VASPs to have in place an AML/CFT program for mitigating ML/FT and PF risks.

The ML/FT and PF risk mitigation mechanism contains various types of documents, methodologies, and analyses regarding business risk assessment, customer onboarding and exit strategies, etc.

The cabinet decision and AML guidelines require DNFBPs and VASPs to document these ML/FT and PF risk mitigation measures deployed in proportion to the risk it is exposed to while considering the findings of the national risk assessment in formal internal documentation, usually known as AML/CFT policy.

These AML/CFT policies and their allied documents, such as procedures and controls, need to be made available to authorities as and when demanded, as the AML Policy substantiates and documents various measures implemented by the DNFBPs and VASPs to curb ML/FT and PF.

## Measures taken for AML/CFT Policy Documentation

Business risk appetite statement, inherent and residual risk analysis

ML/FT risk assessment methodology comprising of risk assessment model, procedure, calculations and risk assessment parameters

Organisational roles and responsibilities for implementing AML compliance tasks

Use of tools for AML compliance and procedure to use such tools and assigning responsibilities and workflows

# The essential elements of an AML/CFT Policy

Documentation of AML policy, procedures, and controls are crucial for the effective and consistent implementation of the AML programs across the organisation. The AML Policy should also be comprehensive, covering the understanding of the law, the customer onboarding process, the reporting requirements, to name a few.

# Essential elements of AML/CFT Policy

01 ML/FT Risk Identification and Assessment

02 Customer onboarding and exit

03 Group-oversight

04 SAR/STR reporting

05 Confidentiality and prohibition against tipping off

06 Staff screening and training

07 Governance

08 Record-keeping

09 Sanctions compliance program

## 1. ML/FT risk identification and assessment

The AML/CFT policy should be formulated using a Risk-Based Approach (RBA), which means that AML/CFT measures must be proportional to the ML/FT and PF risks to which the DNFBPs and VASPs are exposed.

The AML/CFT policy document must enable the staff of the DNFBPs and VASPs to understand and identify the ML/FT typologies according to their sector, such as (virtual assets) VA-related red flags for VASPs, precious stones and metals-related red flags for dealers in precious metals and stones, and the risk factors that expose their business to ML/FT and PF (such as customers, geography, delivery channel, etc.).

The AML/CFT policy must be formulated, considering these risk factors, and the inherent risk must be assessed. The policy must elaborate on qualitative and quantitative risk mitigation measures to reduce the inherent risk, and the procedures and controls to address the same must be outlined.

The AML/CFT policy must clearly state the means or tools relied upon for risk Identification. It must also chart out the tentative organisational roles around risk identification, reporting of suspicious activities and transactions, and tools and procedures relied on for the same. The policy must include imparting staff training for the same and clearly establishing alert escalation and investigation timelines.

**Procedures:**

The procedural part of the policy must address the risk identification and assessment component by setting down steps and procedures for carrying out the enterprise-wide risk assessment that considers business relationship-specific risk, geographic risk, product/service, transaction-based risk, channel-related risk, new technology-related risk, tax crime-related risk, and other risk factors It must also mention risk assessment methodology.

## 2. Customer onboarding and exit

The AML/CFT policy for DNFBPs and VASPs must have clearly outlined instructions regarding the circumstances and timing of conducting following customer onboarding practices:

- Customer due diligence (CDD)
- ID verification process: the tools and solutions used
- Customer risk profiling
- Circumstances necessitating conducting Enhanced Due Diligence (EDD) measures
- Ongoing monitoring of business relationships
- Business relationship handling: in situations where the customer has to be off-boarded or rejected, or an existing business relationship has to be ceased due to a change in the risk profile of such customer or the business relationship or transaction has to be halted
- Conditions and circumstances and extent of reliance on third parties for CDD
- Customer exit policy or situations also need to be elaborated in the AML/CFT policy

## 3. Group-oversight

Group oversight refers to DNFBPs and VASPs having uniform and consistent AML/CFT policies and procedures across their branches, subsidiaries or group companies located in and outside the UAE. The DNFBPs and VASPs in UAE need to ensure that the AML/CFT policies and procedures are consistent with UAE federal laws. The group-wide AML/CFT policies should ideally include the following:

- Procedures for sharing CDD, Know-Your-Customer (KYC), and relevant customer information within the group to seamlessly conduct CDD, risk management, and case management processes and to timely file, report, and record information pertaining to suspicious activities and transactions.
- Transactional involvement in VA transactions across the group or specific branches across the group and compliance with FATF travel rule, where applicable.
- The policy should allow for conducting gap analyses or assessments across its various branches/subsidiaries or group offices worldwide. When the policy cannot be fully implemented, provisions to fulfil or remedy such a situation must be mentioned.
- The AML/CFT policy must contain details of the degree of access managers and employees across the group have to AML compliance tools and systems and tentative workflows for the same.

## 4. SAR/STR reporting

The AML/CFT policies and procedures should ideally contain steps and processes for conducting internal investigation of potentially suspicious activities and transactions by the employees or compliance team to the compliance officer prior to filing official (suspicious activity report/ suspicious transaction report) SAR/STR on the goAML portal. The filing of SAR/STR is a statutory obligation. Failure to report suspicion results in fines and penalties. The AML/CFT policies should ideally contain points discussed as follows:

- The conditions and situations that necessitate managers' and employees' filing of SAR/STRs internally with designated compliance officers and with the regulator, as well as the timing, methods, and formats prescribed for the same.
- Exemption from reporting, if any, to the regulator—If the DNFBP is providing legal services or lawyer services because of confidentiality requirements.
- Procedure for handling business relationships after filing STR by the staff of DNFBPs and VASPs.

Such policies must be communicated to appropriate employees within the organisation, documented and approved by senior management.

## 5. Confidentiality and prohibition against tipping off

The AML/CFT Policies, procedures, and controls must provide for the confidentiality and protection of customer information contained in SARs/STRs. Any suspicion about the customer must not be informed to the customer themselves as it would amount to 'tipping off', which is punishable under UAE federal laws. Appropriate and adequate access rights need to be mentioned in the AML/CFT policy for staff using core AML/CFT systems for case management and defining notification recipients for the same. The AML/CFT policies and procedures must also mention how the flow of information takes place with the regulator. The AML/CFT policy must provide for training to client-facing staff in this regard.

## 6. Staff screening and training

An essential element of AML/CFT policies and procedures for DNFBPs and VASPs is to have defined staff screening and training procedures and requirements in place. Such staff training must ideally include educating the staff about:

- Institutional ML/FT risks;
- The scope of work for customer-facing staff with regard to AML/CFT reporting and internal communications;
- Existing and upcoming ML/FT typologies and new risk factors;
- AML/CFT policies and business procedures.

Such training programs must be based on staff competency, the delivery channel, the training content, and the frequency of training. Ideally, the content of training would differ for the client-facing staff, the compliance team, and senior management, educating each category on the scope of their individual roles and responsibilities to curtail ML/FT and PF. The policy must also discuss how it Identifies, manages, and deploys training resources for its staff.

## 7. Governance

The AML/CFT policies and procedures of DNFBPs and VASPs must contain the governance structure of the business. The AML/CFT policy must provide for the appointment of a competent compliance officer and chart out the responsibilities of senior management, especially regarding granting approvals prior to commencing business relationships with high-risk customers such as Politically Exposed Persons (PEPs). The AML/CFT policy must outline the powers of the audit function with regard to assessing the quality, efficiency, adequacy, and appropriateness of the AML/CFT policy.

## 8. Record-keeping

The AML/CFT policy of DNFBPS and VASPs must ideally contain the scope for maintaining, organising and retaining records and documents pertaining to:

- Roles and responsibilities of client-facing staff, compliance teams and senior management while conducting ML/FT business risk assessments;
- Amendments made to AML/CFT policies;
- Records of AML/CFT compliance events such as:
    - Termination of the business relationship or rejecting a customer due to a change in their risk profile or their name appearing in any of sanctions lists or watchlists;
    - Investigation/inspection/audit records and dates;
- Measures taken for data protection and data privacy;
- Designation of staff for overseeing record-keeping responsibilities such as archiving, cataloguing, maintenance of various registers, and destruction of records exceeding expiry dates such as risk KYC, CDD, EDD, VA transactions, VA wallet addresses, beneficiary and originator details of VA  and transaction records;
- Allocating the appropriate data retention period according to the supervisory body governing the VASPs or DNFBPs.

# Record- Keeping Requirements for Different Locations in UAE

| Location | Applicable to | Supervised by | The prescribed Data Retention Period |
|---|---|---|---|
| **UAE Mainland** | DNFBPs and VASPs | Central Bank of UAE and Securities and Commodities Authority | 5 years |
| **Abu Dhabi Global Market** | DNFBPs and VASPs | Financial Services Regulatory Authority | 6 years |
| **Dubai** | VASPs | Virtual Assets Regulatory Authority | 8 years |
| **Dubai International Financial Centre** | DNFBPs | Dubai Financial Services Authority | 6 years |

**Procedures:**

The types of records needed, customer information, third-party CDD, ongoing monitoring, SAR/STR reports, training logs, etc., must be maintained in given formats.

## 9. Sanctions compliance program

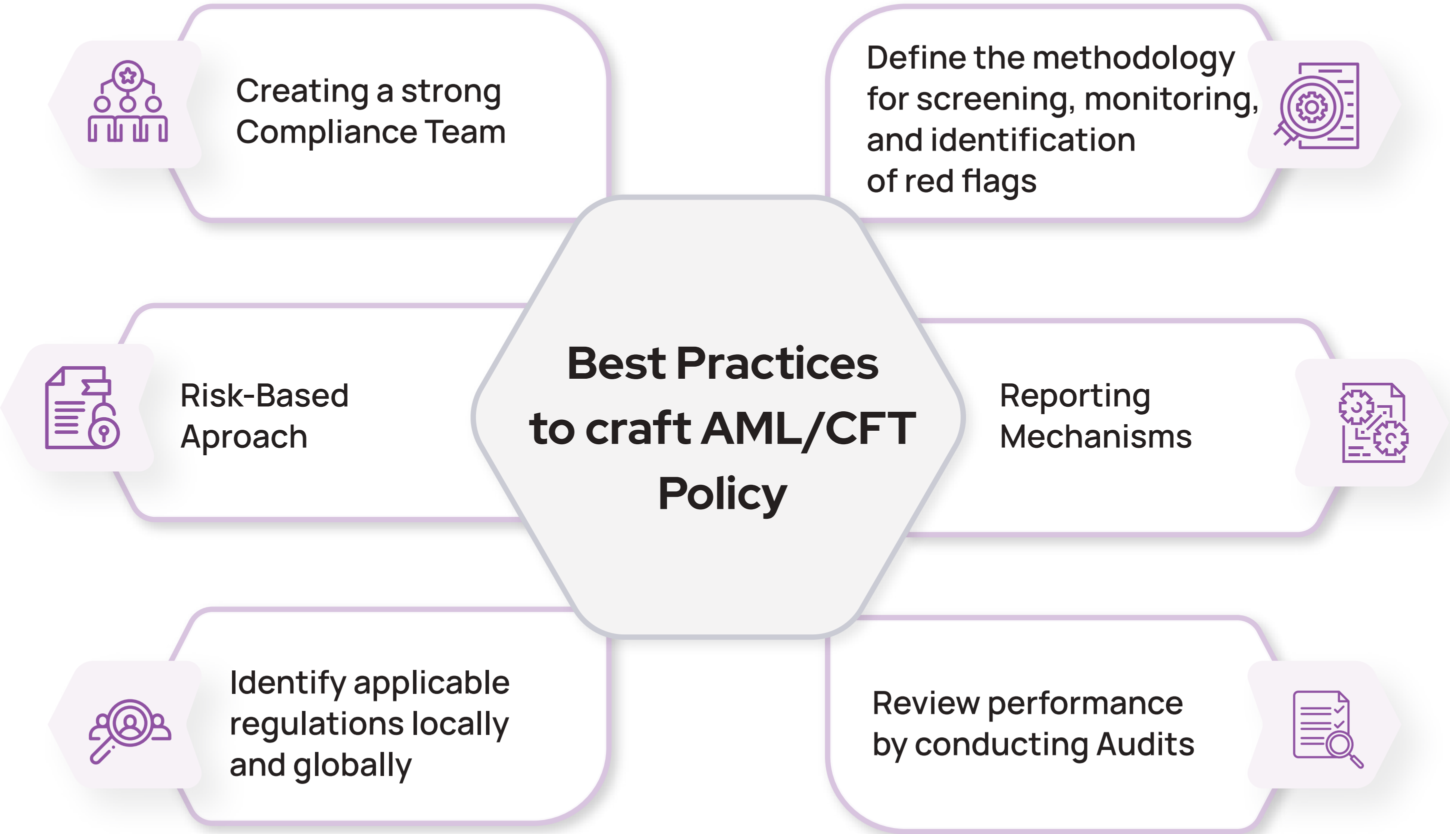
The AML/CFT policy for DNFBPs and VASPs must maintain records of sanctions and targeted financial sanctions lists subscribed.

**Procedures:**

Implementation steps, software tools used, APIs utilised, etc., are to be mentioned in the procedure escalation hierarchy.

# Best practices to craft effective AML/CFT Policy

It is paramount for DNFBPs and VASPs to adopt an effective AML/CFT policy as part of their AML/CFT compliance requirements. For this purpose, they need to keep in mind best practices while formulating the policy that enhances the overall performance of the AML/CFT framework.



Best Practices to craft AML/CFT Policy

Creating a strong Compliance Team

Define the methodology for screening, monitoring, and identification of red flags

Risk-Based Aproach

Reporting Mechanisms

Identify applicable regulations locally and globally

Review performance by conducting Audits

## 1. Creating a strong compliance team

To create an effective AML/CFT policy, the DNFBPs and VASPs need to ensure that their team of compliance personnel is competent to develop an AML/CFT policy that is adequate and proportional to their business's exposure to risks. The compliance team must be strong and well-versed in the latest trends and amendments in the UAE federal laws and international regulations for curbing ML/FT and PF.

Having a strong compliance team will ensure the effective implementation of the AML/CFT policy and the timely, effective, and accurate fulfilment of the AML/CFT obligations of DNFBPs and VASPS.

## 2. Risk-based approach

The AML/CFT policy for DNFBPs and VASPs must be crafted by taking into consideration the various kinds of ML/FT and PF risks to which the business is exposed. The AML/CFT policy must be just right for the business; it should not be overly stringent, leading to difficulty in conducting business and higher costs, nor the AML/CFT policy should be under-compliant, leading to cracks or loopholes that criminals can take advantage of while conducting business with such DNFBP or VASP.

Ideally, the AML/CFT policy needs to be the perfect blend of adequate compliance measures, considering a variety of risk factors, each identified, assessed and mitigated appropriately.

## 3. Identify applicable regulations locally and globally

The AML/CFT policy must be crafted while considering the crucial component of ensuring adequate compliance with applicable laws and regulations, both on a local and international basis.

The DNFBPs and VASPs need to consider the applicable supervisory authority and rules issued in regard to curbing ML/FT/PF, such as the DFSA, ADGM, or VARA. At the same time, the DNFBPs and VASPs should also consider the laws of other countries in which they are operating and the relevant AML/CFT measures prescribed. Whether such measures are at par with FATF standards or not should be considered, and if such measures are sub-standard to FATF recommendations, the DNFBPs and VASPs must formulate their policies by covering for these deficiencies for their branches, subsidiaries, and third parties operating outside UAE.

## 4. Define the methodology for screening, monitoring, and identification of red flags

The AML/CFT policy crafted is only as effective as the processes, methodologies, steps and measures prescribed within. The AML/CFT policy needs to clearly define the manner in which the business is required to conduct various kinds of name screening, ongoing monitoring and identification of AML/CFT typologies. The DNFBPs and VASPs must also seriously consider relying on AML/CFT software, automation tools, APIs, etc., to reduce costs, streamline compliance and operational processes, automate mundane and repetitive tasks, and send alerts when any red flags are identified.

## 5. Reporting mechanisms

The effectiveness of an AML/CFT policy is usually gauged by its ability to educate and enable customer-facing staff, compliance officers, and senior management to actively participate in identifying suspicious activities or transactions related to ML/FT and PF. The AML/CFT policies, procedures, and controls must provide the formats, escalation methods, and internal reporting mechanisms and steps prior to the official filing of SAR/STR and define timelines on the goAML portal.

## 6. Review performance by conducting audits

The effectiveness and accuracy of the AML/CFT policy in the context of its compliance with regulatory requirements can be assessed only by conducting frequent and unbiased AML/CFT policy audits. An Independent audit function must conduct such audits to test the efficiency, adequacy and accuracy of internal policies, procedures, and controls. If any deficiencies are found, senior management must remedy such deficiencies as soon as possible.

# AML/CFT Policies are incomplete without the **procedures**

AML/CFT Policies are official documents that establish internal rules for the business to follow for ensuring continuous compliance with relevant laws.

AML/CFT Procedures define and state the individual roles and responsibilities to ensure that the policies' provisions are complied with in totality. They also prescribe the use of tools, software, or mechanisms to establish and ensure control over policies and procedures. In simple terms, policies establish internal rules and procedures specify who shall do what task and in what manner.

AML/CFT procedures clarify the management objectives and processes involved in ensuring compliance with the AML/CFT policy.

AML/CFT procedures clarify and shape employee conduct and behaviour in accordance with the AML/CFT policy by setting the tone of how compliance processes and activities shall be carried out within the organisation.

The procedures govern how compliance with the policy is achieved; for example, defining the steps for performing the name screening process and elaborating on the methodology and tools used for name screening would aid with compliance with policy requirements related to name screening. The procedures would contain a step-by-step guide on how to conduct name screening, which tool to use, how to record and report various outcomes, when and to whom to escalate the case, etc. The AML/CFT policies are incomplete without the procedures that map out the steps to be carried out by the staff of the business to ensure its compliance with regulations as given in the policy.

# AML/CFT Policies are incomplete without the procedures

## AML/CFT Policy

- Consists of internal rules aligned with regulatory requirements
- Scope is Company or Group-wide
- Contains to-do’s and do-not’s
- Defines stance of company towards regulatory compliance

## AML/CFT Procedures

- Consists routine practices to supplement internal rules
- Scope is limited to specific tasks and activities such as sanction screening, CDD, KYC or EDD. etc.
- Contains step-by-step approach with escalation and completion timelines
- Defines employee conduct in alignment with company stance

# Conclusion

Crafting effective AML/CFT policies, procedures, and controls to achieve adequate ML/FT and PF risk mitigation is an essential requirement for DNFBPs and VASPs operating in the UAE.

AML/CFT policies, procedures, and controls are to be carefully drafted, keeping in mind the individual business needs according to the nature and size of operations, the industry-specific AML/CFT compliance requirements (such as VASPs, Real-Estate, Gold sector, Legal services providers, etc.), and region/supervisory body-specific AML/CFT rules (such as DFSA, FSRA, VARA, etc.). The AML/CFT policy for VASPs and DNFBPs would differ significantly according to their respective AML compliance requirements. However, the fundamental requirements of adherence to federal laws offer certain uniformity, as discussed in the booklet above.

The AML/CFT policies, procedures, and controls should ultimately ensure relevance to the business for which they are being crafted to adequately mitigate ML/FT and PF risks.

# About RapidAML

**RapidAML is an AML software designed to support the compliance tasks of the DNFBPs and the VASPs, offering an advanced and secured technology platform**

## Who we are

Facctum, founded in 2021 by a group of enthusiasts who have experience in banking, financial crime risk management technology, data science, etc., specialises in building risk management solutions with new-age technology.

## Our Mission

We understand the significance of AML compliance and recognise its complexity. Addressing this issue is our mission at RapidAML.

Our solution focuses on simplifying the intricate regime of AML compliance with advanced technology. We aim to help the regulated entities, specifically the DNFBPs and the VASPs, smoothen their AML efforts with RapidAML's end-to-end AML software.

## Our Vision

Our vision is to develop next-gen AML software that offers an affordable and complete solution to all the AML compliance-related issues of every DNFBP and VASP worldwide.

## Our Core Values

We live by these guiding principles that guide our progress

### Customer Focused

We are committed to offering quality AML support to exhibit a constructive effect on the customer's business

### Elevated Excellence

With a comprehensive, tech-driven financial crime compliance solution, we nurture customer's efforts and ignite brilliance to AML function.

### Innovation Is The Key

We strive for healthy competition, bringing out the best version of the AML tools and technologies with continuous research and improvement.

### Integrity

We value our customers, our team, and our society, and we build trust with our committed honesty and transparency.

### Together We Win

With inclusiveness and a sense of collaboration, we assist our customers in accomplishing compliance and developing a sense of shared achievement.

RapidAML

www.rapidaml.com

info@rapidaml.com

Follow us on: