RapidAML

Mitigating Money Laundering Risks:

Strategies for DNFBPs and VASPs

www.rapidaml.com

info@rapidaml.com

RapidAML

Money laundering is a global risk that affects Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers. Mitigating money laundering risk is the top priority of regulators and the regulated entities. Here is the article providing insights into various strategies that entities can adopt to mitigate money laundering risks.

www.rapidaml.com

info@rapidaml.com

RapidAML

Table Of Content

Money laundering risks and the role of DNFBPs and VASPs

Money laundering usually involves illegally acquired money, often termed “black money” or “dirty money,” being concealed, disguised, moved, rotated, or exchanged amongst several hands to wash off the traces of its origin, which is generated from criminal activity. This process of washing off the traces of the origin of black money is known as money laundering.

Why do people launder money

Money laundering is carried out with the intention of avoiding suspicion or detection by law enforcement agencies to avoid conviction, imprisonment, fines, and freezing or confiscation of such illicit funds.

Further, criminals also intend to launder money for the following reasons:

- To disguise the source of illegal funds.
- To evade taxes and financial regulations.
- To fund further criminal activities.
- To legitimise proceeds from illegal activities for personal use or investment.

What is Money Laundering Risk

Money laundering risk refers to the probability that criminals could misuse legal or natural persons as a channel to carry out their illegal activities. Designated Non-Financial Businesses and Professions (DNFBPs) and Virtual Asset Service Providers (VASPs) must identify, assess, and understand the money laundering (ML) risk to mitigate it effectively.

The Stages of Money Laundering

DNFBPs and VASPs need to ensure that their business is not used as a medium to conduct money laundering activities by money launderers as they are prone to be misused by launderers due to the nature of their business, which involves multiple geographies and modes of transactions, complex business structures, products, and services across various jurisdictions.

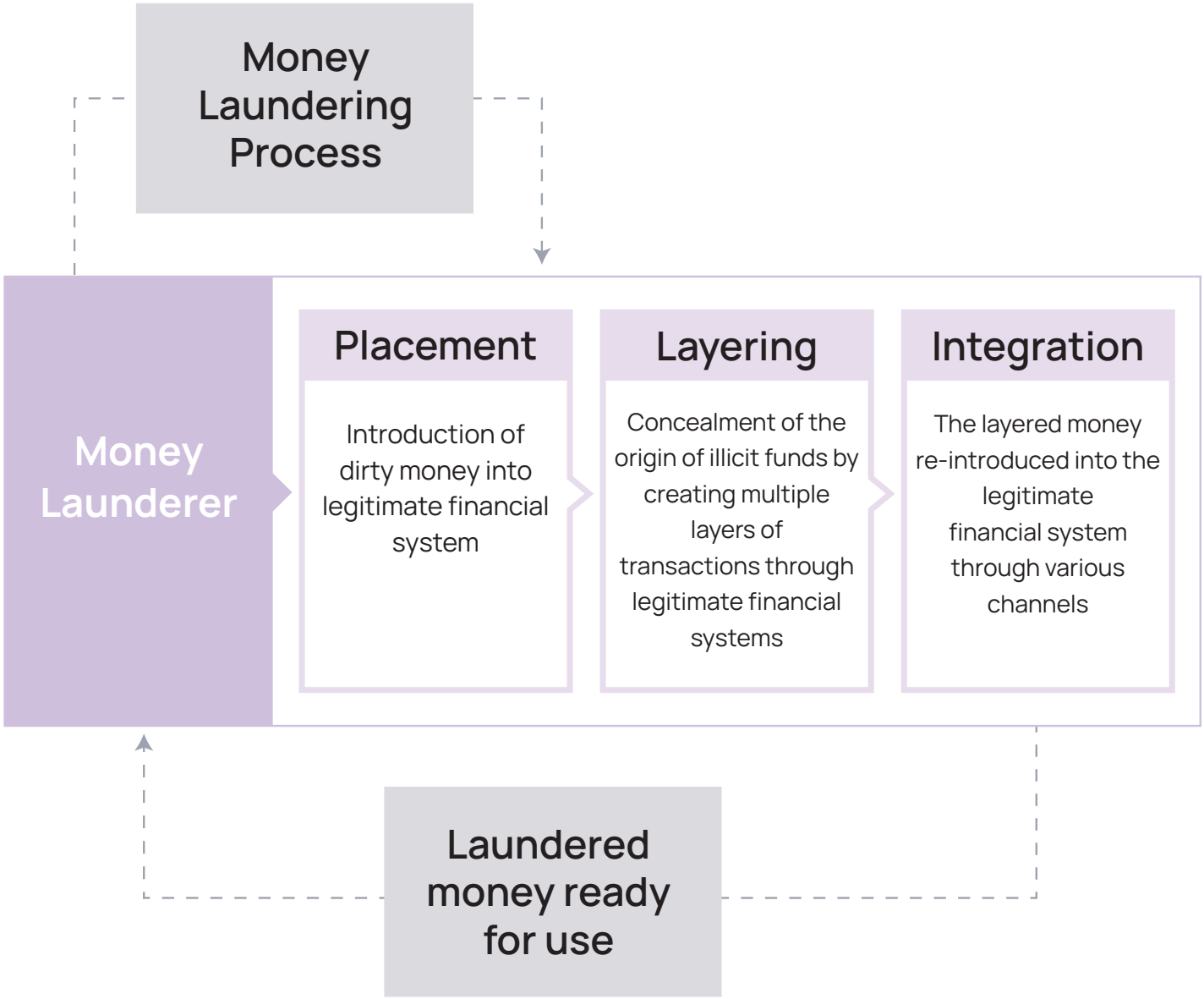
The crime of money laundering is executed in three stages, known as placement, layering and integration.

1. The **placement** stage is the first stage of money laundering. It involves introducing the proceeds of crime into the financial system. The placement stage denotes the entry of "dirty money" into the legitimate financial system by freeing up the criminal holding and storing illegal cash.

2. Next comes the **layering** stage. At this stage, dirty money or black money is distanced from its source. Measures are taken to conceal its original source by creating multiple transactions and fund transfers, usually by creating multiple layers or series of transactions to avoid detection of the origin of funds, making the dirty money look as if it was earned through legitimate sources of income. In the layering stage, the illicit proceeds make their way into the banking and financial institutions where their paper trail gets created, thus making it very difficult to identify their true source. Layering is also known as structuring because, as the name suggests, large sums of illicit funds are split into a series of smaller transactions that do not catch the attention of authorities and are spread across multiple accounts.

3. The final stage in the money laundering process is the **integration** stage. In this stage, the layered funds are integrated into the financial system, which the launderer can use for legitimate purchases and investments or to carry out criminal activities by carrying out transactions that seem to be legal.

The Stages of Money Laundering



Red Flags and Indicators of Money Laundering

The best way to ensure that DNFBPs and VASPs can safeguard themselves from money laundering is to ensure that all relevant personnel of the DNFBPs and VASPs are made aware of the money laundering and financing terrorism (ML/FT) risk indicators or ML/FT red flags.

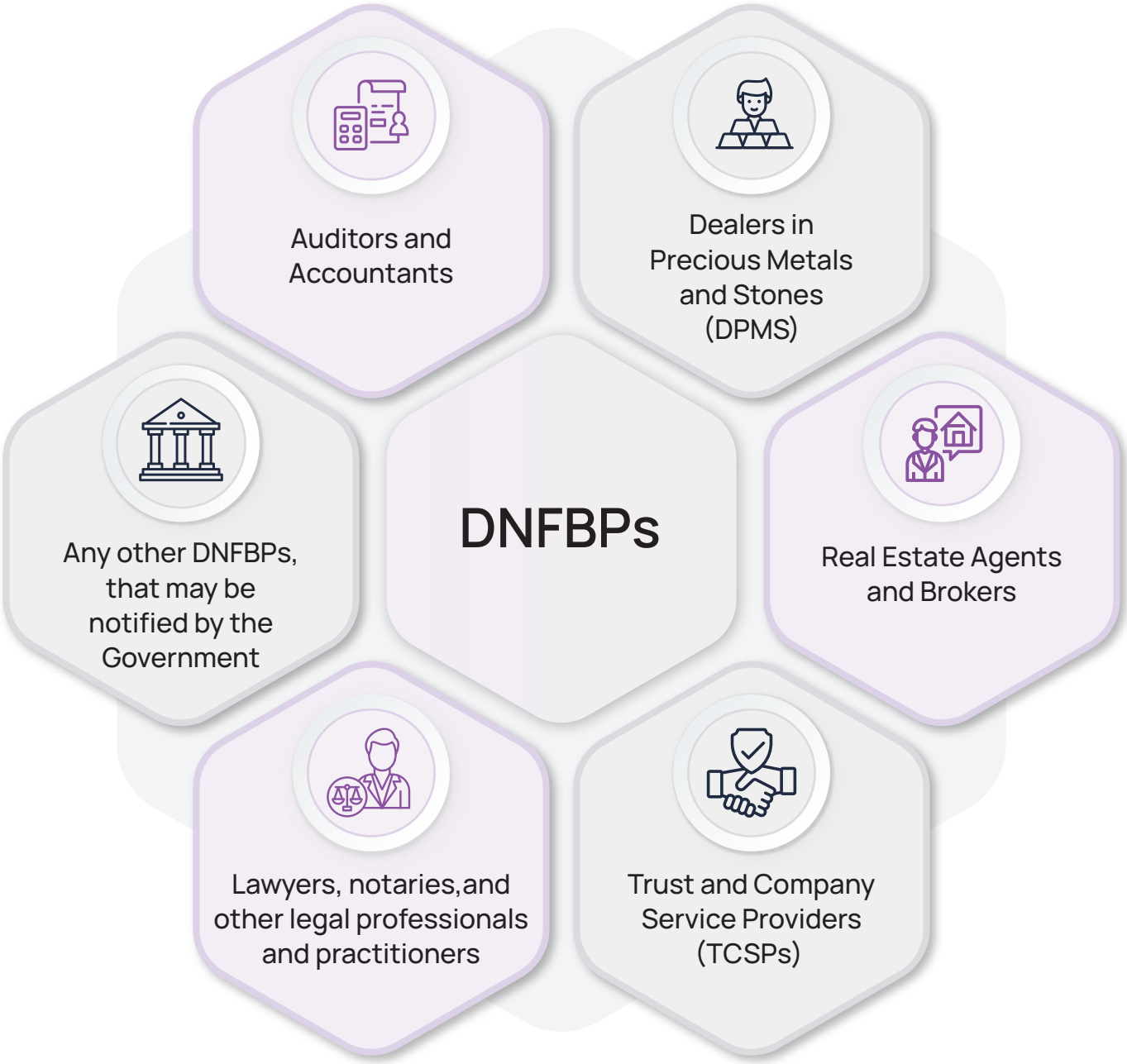
These ML/FT risk indicators can be broadly classified into the following categories, with some of the examples of such red flags, including but not limited to:

Customer related Red-Flags	Relating to the behaviour, conduct, degree of cooperation, nature (i.e., a natural person or legal person, Politically Exposed Person, high-risk customer or belonging to a high-risk country), nationality, chosen mode of payment, sources of funds, and wealth of such customer.
Transaction-related red flags	Relating to the mode of transaction such as wire transfer, use of virtual assets, money value transfers, involvement of third parties, unusually short payment cycle, or insistence on the use of cash payment for high-value transactions.

The Role of DNFBPs in Countering Money Laundering

Designated Non-Financial Businesses and Professions (DNFBPs) are those entities or businesses that are involved with the various commercial activities.

Categories of DNFNPs under UAE's AML Regulations



Why DNFBPs are Vulnerable to Money Laundering

DNFBPs are vulnerable to money laundering because, being a non-financial sector, they are not regulated as strictly as the banking and financial sectors are. DNFBPs are exposed to ML/FT and risks arising out of the following reasons:

- Dealing with customers from various countries, some of the countries are blacklisted by the Financial Action Task Force (FATF) for not having implemented adequate AML/CFT and CPF measures and promoting nuclear funding and grey listed for having weaker AML/CFT and CPF controls, the DNFBPs need to be mindful about the customer's country they are dealing with;
- Non-awareness of customer due diligence practices and tools to detect potentially fraudulent or criminal activities that promote ML/FT and PF;
- The non-monitoring of existing customer relationships leads to the creation of a blind spot from where ML/FT or PF risks might enter the business.

Example of DNFBP's vulnerability to money laundering:

Money launderers can buy, hold, or sell high-value diamonds and liquidate them in any country, transport those easily, escaping the scrutiny of authorities to conceal the illegal origin of dirty money and proceed with structuring and integration.

The Role of VASPs in Countering Money Laundering

Virtual Asset Service Providers (VASPs) are businesses that are engaged in Virtual Assets or “VA” services. VAs include digital representations of amounts that have a digital existence and can be traded or transferred digitally or utilised for payment or investment purposes. Examples of VAs include bitcoin, dogecoin, and ether. Virtual Assets do not include fiat currencies, shares, securities, or other e-money instruments.

VASPs conduct one or more operations on behalf of a company or individual, such as:

- Exchanging virtual assets and fiat currencies
- Exchanging across one or more forms of virtual assets
- Transfer of VA from one virtual asset address to another virtual asset address
- Safekeeping, administration, and control of VA assets
- Participation and provision of financial services related to the sale or offer of virtual asset

Unique Money Laundering Risks Associated with VASPs

VA activities and VASPs are prone to high ML/FT and PF risk due to their basic nature: easy access to the Internet, offering anonymity while dealing with virtual assets. This anonymity feature attracts criminals who want to avoid scrutiny under usual channels when carrying out their transactions.

The unique ML/FT risks associated with VASPs are as follows:

- No awareness or insufficient implementation of the FATF travel rule; that is regarding the collection of the VA transaction's originator and beneficiary information;
- Lack of knowledge and subject expertise when it comes to implementing adequate ML/FT measures, particularly tailored for VASPs;
- Risks arising from centralised and decentralised VASP business models;
- Unique VA services such as tumblers or embedded mixers that undermine the VASP's ability to acquire adequate customer due diligence (CDD) and know your customer/transaction information (KYC/KYT);
- Unique ML/FT risks due to unique business model;
- The platform or medium through which the VASP operates, such as the trading platforms, peer-to-peer exchanges or kiosk-based exchanges, each pose distinct ML/FT risks;
- VASP's exposure to IP address anonymisers that disable the VASPs to conduct CDD adequately;
- VASP's association with risky jurisdictions;
- The nature and scope of VASP payment modes or systems such as open-loops, closed-loops or micro-payment;

A Risk-Based Approach to Mitigating Money Laundering Risks

The UAE federal laws and FATF recommendations require DNFBPs and VASPs to implement a risk-based approach (RBA) to mitigate their exposure to ML/FT risks. The RBA consists of measures, systems, and controls that are specifically designed to identify, assess, mitigate, and address the ML/FT risks that differ from business to business.

Why a One-Size-Fits-All Approach to AML doesn't Work

The one-size-fits-all approach while implementing the RBA is not effective as ML/FT risk exposure will differ from business to business as each business, be it DNFBP or VASP, is unique and distinct in terms of their business model, risk factors such as customers, geographies, delivery channels, use of technology, tax regimes, sanctions requirements, or potential events of sanctions evasions. The identification of inherent risks, risk appetite, and assessment of residual risk would differ from business to business, which would cause every business's RBA component to be different. Also, relying on a one-size-fits-all approach would lead to over-compliance or under-compliance of AML/CFT measures.

Importance of Identifying Risk Levels for Customers and Transactions

One important element of the RBA is customer and transaction risk profiling, which evaluates the risk levels of customers and transactions. The process of assigning risk levels involves:

- Identifying the ML/FT risk factors that a particular customer or transaction poses to the business;
- Weighting of various ML/FT risk factors identified for each customer or transaction;
- Assigning risk levels or risk classification by having a benchmark derived from generic customer profiles of similar type;
- Documenting the risk assessment process.

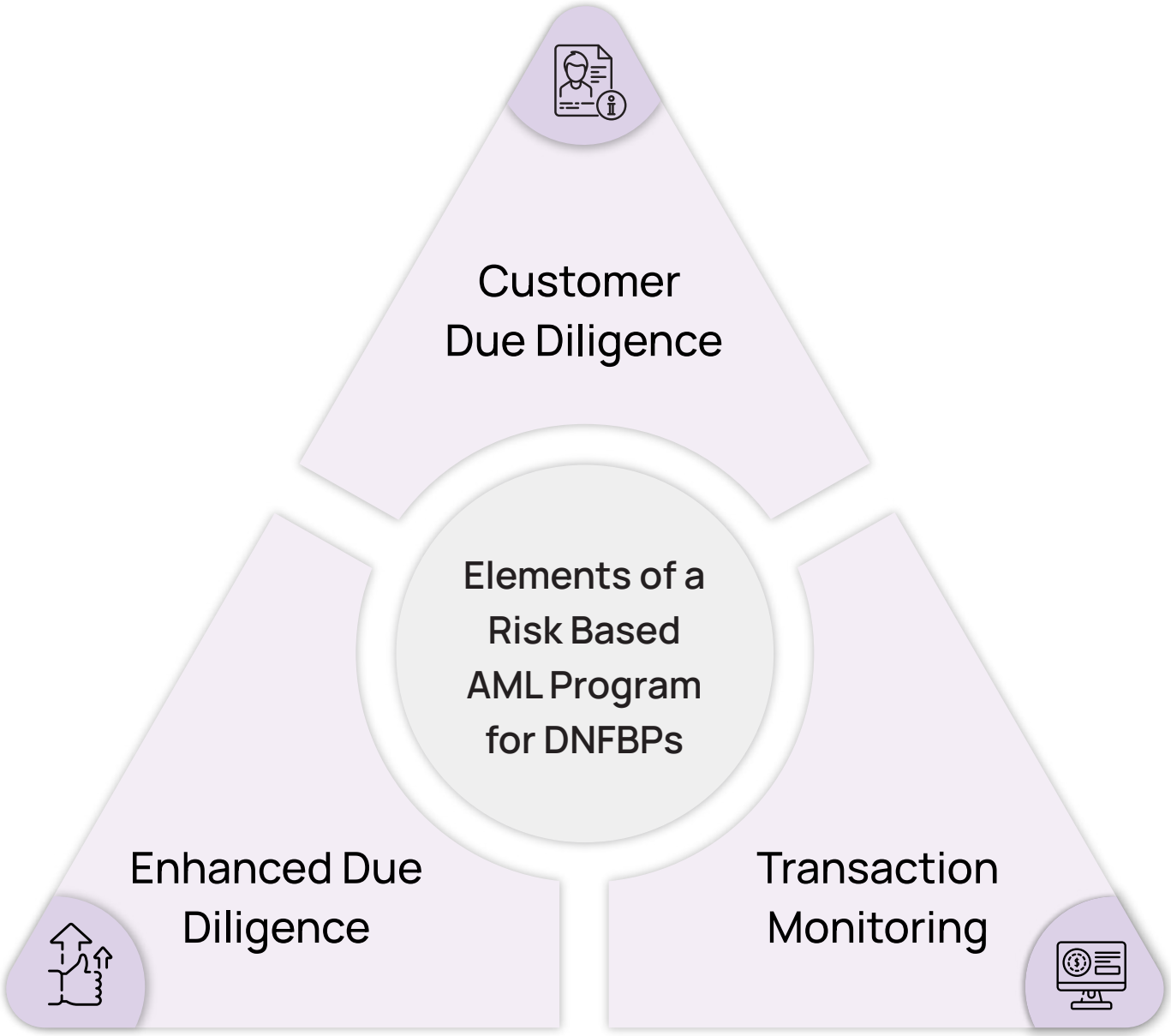
Having identified the risk levels for customers and transactions would enable the DNFBPs and VASPS to have a clear idea about the level of risk posed by each customer and transaction and the degree of risk mitigation measures to be applied for that particular customer or transaction, which is applying Enhanced Due Diligence Measures for high-risk customers or Simplified Due Diligence Measures for low-risk customers, resulting in an effective and robust AML/CFT compliance measures.

Implementing a Risk-Based AML Program for DNFBPs

A risk-based AML/CFT program for DNFBPs is essential to ensure that their internal policies, procedures, and controls of the DNFBPs are in accordance with the requirements of the UAE federal law and are up to the standards recommended by the FATF. The risk-based AML/CFT program helps the DNFBPs to take adequate due diligence measures while considering the findings of the national risk assessment and the other relevant risk factors.

An ideal risk-based AML/CFT would consist of three major elements, that are Customer Due Diligence, Transaction Monitoring and Enhanced Due Diligence.

Essential elements of DNFBPs risk-based AML program



Customer Due Diligence (CDD)

Risk-based Customer Due Diligence measures contain steps and processes such as follows:

- Steps and procedures for identifying and verifying the customers that are legal and natural persons; beneficiaries and persons controlling the legal persons, ultimate beneficial owner (UBO) of the legal entity customer based on information provided by them across reliable sources;
- Steps and procedures for carrying out the name screening of customers to identify if such a customer is high-risk, belongs to any high-risk country, is a Politically Exposed Person (PEP), or has their name appearing across any of the international sanctions lists;
- Having a requirement in place for identifying the nature and purpose of prospective business with a customer, particularly when such customer is a legal entity, details about its control structure and control percentages;

- Having measures, tools, procedures, and controls in place that enable the DNFBPs to monitor their existing customers on an ongoing basis;
- Having measures in place that assess the transactions taking place throughout the course of the business relationship to ensure consistency of such transactions with the purpose of the business relationship;
- Having the documentation, cataloguing, and archiving process in place to ensure compliance with the AML/CFT record-keeping requirements.

Further, the factors to be considered while conducting risk-based CDD are:

- The results of ML/FT and PF enterprise-wide risk assessments/business risk assessments;
- The situations, appropriate timing and steps and procedures for implementation of CDD measures;
- Periodicity and timelines for reviews, changes, and updates in customers' CDD information;
- Periodicity and timelines for conducting ongoing monitoring of business relationships.

Enhanced Due Diligence (EDD)

As the name suggests, Enhanced Due Diligence refers to CDD measures with increased intensity and level of scrutiny, such as:

- Having measures in place for increased verification and documentation from reliable sources to verify customer information;
- Having steps and processes for carrying out a detailed inquiry about the reason behind establishing business relationships and ascertaining if the profile of the customer is consistent with the customer's sources of funds and sources of wealth;
- Having measures in place for obtaining senior management approval prior to onboarding high-risk customers, a higher frequency of monitoring, reviewing and updating of CDD information and transactions.

The risk-based AML/CFT policies, procedures, and controls must contain details of:

- Situations that require the carrying out of EDD measures;
- Define the periodicity of carrying out reviews and updating information about high-risk customers;
- Degree of depth and periodicity in conducting ongoing monitoring of high-risk business relationships.

Transaction Monitoring

Transaction monitoring is an essential element of a risk-based AML program. DNFBPs are required to have their policies, procedures, and controls in alignment with enterprise-wide risk assessment and have measures in place to identify, list out, and have processes in place to assess potentially suspicious transactions.

The senior management of the DNFBPs must approve the risk-based AML/CFT program and AML/CFT policies and procedures, and they must also oversee the onboarding of high-risk customers with their approval. The DNFBPs need to appoint a competent Compliance Officer who can supervise AML/CFT compliance requirements. Customer-facing personnel and relevant personnel must be adequately trained to implement the risk-based AML/CFT program effectively.

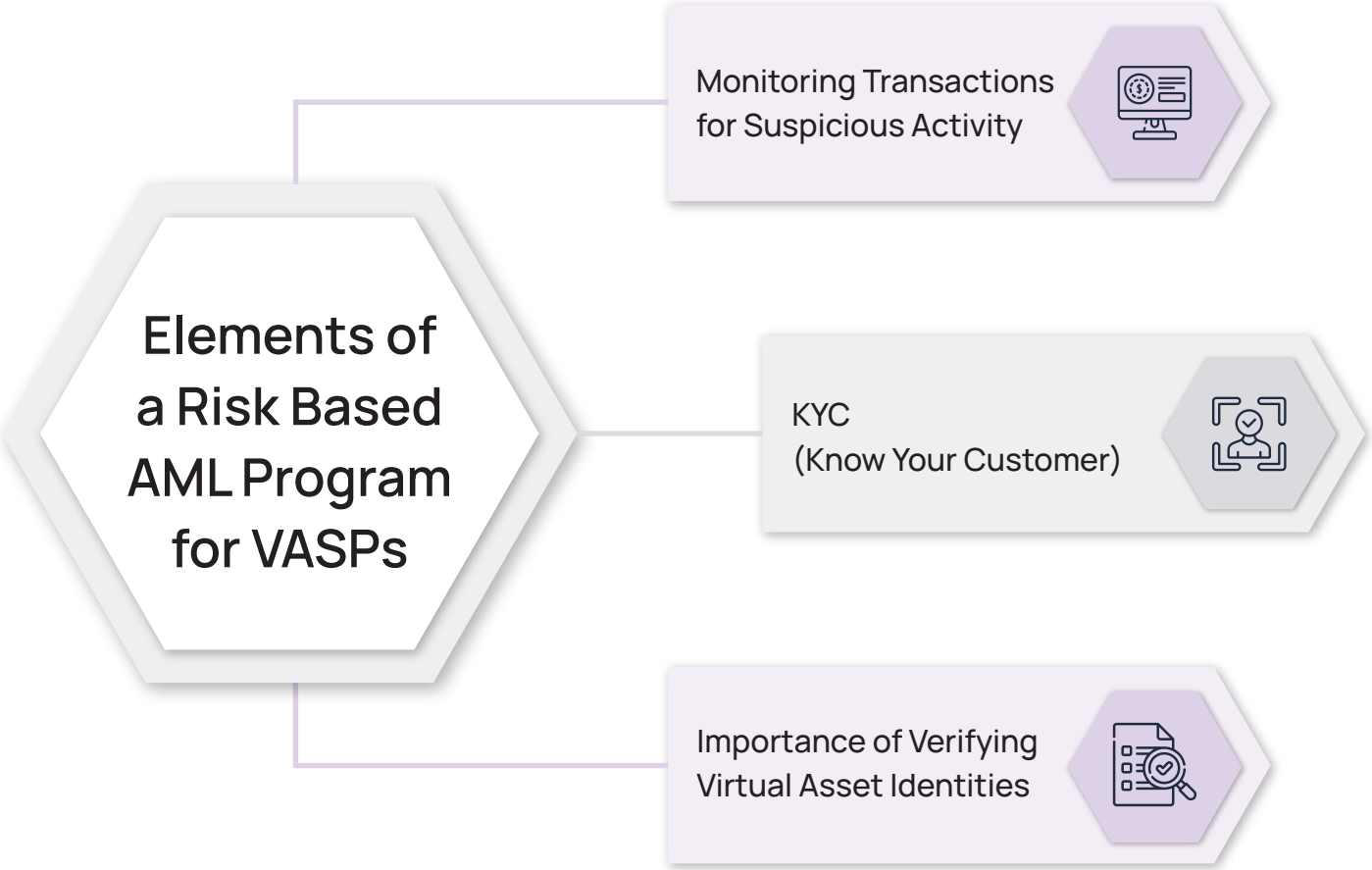
Implementing a Risk-Based AML Program for VASPs

VASPs need to formulate a risk-based AML/CFT program to ensure compliance with UAE federal laws and the FATF recommendations.

The risk-based AML/CFT program helps the VASPs to take adequate due diligence measures while considering other relevant risk factors.

An ideal risk-based AML/CFT would consist of three major elements, that are KYC (Know Your Customer), the importance of verifying virtual asset identities and monitoring transactions for suspicious activity.

Essential elements of VASP's risk-based AML program



KYC (Know Your Customer) for VASPs

The authorities encouraged VASPs to rely on technological solutions to conduct the CDD process. The Know Your Customer (KYC) process for VASPs can include the use of tools that facilitate verifying and confirming their customers' identification by clicking or uploading selfies using the customer's own cell phones to authenticate their identity.

VASPs are also required to screen their customers across various international sanctions lists with the VA and VA wallet addresses. As a part of adequate CDD requirements, VASPs need to include the beneficiary account details, along with the originator account details, their respective IP addresses and wallet addresses. These details should be monitored on a regular basis.

Importance of Verifying Virtual Asset Identities

VA identities need to be verified to ensure compliance with the UAE federal laws and to mitigate ML/FT risks to which the VASPs are prone. The process of identifying and verifying VA identities helps VASPs in the following ways:

- Collection and verification of important information about customers helps in identifying risks, such as their geographical risks and transaction pattern risks;
- Collection and verification of VA information will help in identifying the nature and purpose of the proposed VA transaction;
- Collection and verification of VA information helps in establishing the legitimacy of the VA customer and documenting the CDD carried out for VASPs;
- Collection and verification of VA information helps streamline the customer onboarding process by using verification measures such as facial recognition;
- VA documentation verification process helps in identifying fraudulent and fake documents and information;
- VASPs efficiently conducting VA collection and verification of VA information can reduce the risk of AML/CFT violation fines and penalties.

Monitoring Transactions for Suspicious Activity

VASPs need to have a risk-based AML program with steps and procedures in place that enable VASPs to monitor their customer relationships by identifying, evaluating, and reporting suspicious activities and transactions to the Financial Intelligence Unit (FIU) through the goAML portal. The VASPs AML/CFT program should contain ML/FT typologies relevant to VASPS along with red flags of ML/FT that help the personnel of VASPs become aware of red flags.

Building a Robust AML Compliance Framework

The ML/FT and PF risks for DNFBPs and VASPs and the UAE federal laws require building a robust and effective AML Compliance framework. A robust AML compliance framework helps to effectively navigate the intricacies of the legal framework and further facilitates compliance with the regulatory requirements.

Key elements of an effective AML Compliance Framework

AML Compliance Framework

1. Establishing a Strong AML Culture
2. Training and Awareness Programs for Staff
3. Record-Keeping and Reporting Requirements
4. Internal Controls and Risk Management Processes
5. Utilising Technology to Enhance AML Compliance
6. Transaction Monitoring Tools
7. Customer Identification and Verification Systems

Establishing a Strong AML Culture

Any AML compliance framework is only as effective in combating ML/FT and PF as the type of compliance culture that exists within the DNFBPs and VASPs. The Senior Management is responsible for setting the tone of the AML compliance culture, as they are the top management. The employees of the DNFBPs and VASPs need to be educated about ML/FT and PF typologies relevant to their organisation and encouraged to report to the compliance officer. The compliance officer is responsible for reporting suspicious activities and transactions to the FIU (Financial Intelligence Unit) and ensuring that the AML/CFT program, policies, and procedures are implemented across the organisation.

Training and Awareness Programs for Staff

The AML/CFT framework of DNFBPs and VASPs needs to provide for the training of their relevant employees (customer-facing staff, compliance officer, and senior management) regarding ML/FT red flags, ML/FT typologies, ML/FT reporting, and record-keeping requirements to ensure that they are well aware of their individual responsibilities towards preventing ML/FT and PF incidences.

Record-Keeping and Reporting Requirements

The AML compliance framework of DNFBPs and VASPs needs to provide for documenting their AML compliance procedures and policies and maintain records of the customer information derived during the CDD, EDD, AML training logs, training attendance lists, Risk assessment methodologies and outcomes, internal suspicious activities reports and transactions for the period prescribed by their supervisory body.

Internal Controls and Risk Management Processes

The AML framework for DNFBPs and VASPs needs to contain the processes that they undertake to control the ML/FT and PF risks. The risk management process includes steps taken to identify, assess and mitigate ML/FT and PF risks the business is exposed to, such as enterprise-wide risk assessments where the risk mitigation is done on the basis of various risk factors such as customers, geographies, transactions, delivery channels, and so on.

Utilising Technology to Enhance AML Compliance

The AML framework of DNFBPs and VASPs needs to include the details of the technology they rely on while conducting AML compliance processes, as the use of AML software solutions is encouraged by federal laws. DNFBPs and VASPs may rely on several AML solutions, such as name-screening software, customer onboarding and risk assessment tools, and case management tools, while ensuring that such tools are compliant with regulatory requirements.

Transaction Monitoring Tools

The AML framework must provide details of the transaction monitoring tools relied upon by the DNFBPs and VASPs. Transaction monitoring is essential to identify any deviation or change in the customer profile during the course of the business relationship. The deviations, changes, or updates to a customer's profile are alerted by the transaction monitoring tool to the user, usually the compliance team or customer-facing team, enabling them to take corrective action such as requesting additional or fresh information or filing suspicious activity or suspicious transaction reports.

Customer Identification and Verification Systems

The AML compliance framework needs to include the details of customer identification and verification systems relied upon and ensure that adequate record-keeping measures are taken to document the customer identification and verification details of each customer that the DNFBPs or VASPs intend to onboard. The customer identification and verification systems will help the DNFBPs and VASPs ensure that the CDD and EDD requirements of the UAE federal laws are adequately complied with.

Conclusion: Protecting Your Business and the Financial System

The DNFBPs and VASPs operating in the UAE need adequate ML/FT risk identification and assessment mechanisms to effectively mitigate ML/FT risks by educating their relevant personnel about the ML/FT typologies, building strategies and AML/CFT compliance framework based on a risk-based approach where the risk mitigation measures are applied in proportion to the risks to which their individual businesses are exposed.

The senior management and compliance officers of DNFBPs and VASPs also need to remember that ML/FT risk assessment is unique for each business, and a one-size-fits-all approach cannot be relied upon while implementing risk mitigation mechanisms.

ML/FT risk mitigation needs to be carefully tailored to fit the AML/CFT compliance needs according to the nature, size, sector, area of operations, number and types of customers, volume of business, and desired modes of transaction, which varies from business to business. However, the generic requirements of the robust AML compliance framework are discussed to update the DNFBPs and VASPs on the basic requirements of the UAE federal laws and FATF recommendations.

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.

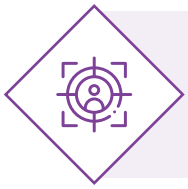
Our solution focuses on simplifying the intricate regime of AML compliance with advanced technology. We aim to help the regulated entities, specifically the DNFBPs and the VASPs, smoothen their AML efforts with RapidAML's end-to-end AML software.

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

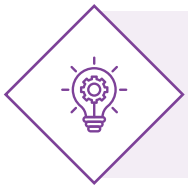


Customer Focused

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.

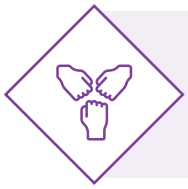


Innovation Is The Key

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: