

Combating **Crypto** **Money Laundering** with

Risk-Based AML Compliance

Table of Contents

Introduction	1
Why is Crypto Money Laundering Attractive to Criminals?	3
How does Crypto Money Laundering occur?	6
What are the Red Flags of Crypto Money Laundering?	11
How to Combat Crypto Money Laundering?	13
FATF Recommendations Concerning VASPs	15
FAQs on Crypto, VASPs and Its Regulating Authorities	18
How can AML UAE Assist you in AML Compliance?	21
About AML UAE	23





Introduction



Money laundering is on the rise globally.

Money launderers and financial criminals are increasingly exploiting technological advancements to conduct financial crimes.

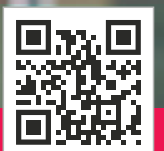
They are misusing loopholes in regulations and technology to find out new ways of placing and layering illicit money. And the latest victim of their laundering attacks is the world of virtual assets and cryptocurrency.

ADDITIONAL INFORMATION & RESOURCES

-  AML Compliance Calendar
-  Virtual Assets AML Compliance eBook
-  Additional AML Obligations of VASPs: KYT and KYV
-  Virtual Assets Regulatory Authorities in UAE
-  Navigating the concept of Virtual Asset and VASP (Virtual Asset Service Provider)
-  Navigating CDD and FATF Travel Rule: VASPs to identify Originator
-  AML Compliance Journey for VASPs in UAE
-  AML regulations for Virtual Asset Service Providers in UAE



Why is Crypto Money Laundering Attractive to Criminals?





Inadequate or No Regulation

The absence or lack of controls and regulations on cryptocurrencies is the primary reason for a rise in crypto money laundering. Many laws and rules exist for other financial channels, currencies, and instruments, wherein fines and penalties are imposed for non-compliance with these laws.

However, these are not currently prevalent in regulating the world of cryptocurrencies. Since it is a new form of currency, not yet acceptable in all countries, it is not adequately regulated by most countries. There are no centralized authorities involved in crypto transactions. Money launderers are attracted to crypto assets, as loose regulations result in a higher scope of not being caught by authorities.



Anonymous in Nature

Generally, individuals do not have to share their names while dealing with cryptocurrencies. Public addresses are used in these transactions, which do not relate to the user's name. It provides users with a degree of anonymity, which is what makes cryptocurrencies desirable to money launderers.

There is no paper trail of a transaction. Only a digital record exists on the distributed ledger technology. Therefore, it is easier for criminals to move large amounts of illicit funds through blockchain technology without disclosing their identity.



Fast and convenient

The processing of cryptocurrencies occurs through online exchanges. These online transactions can happen across borders without many protocols. Thus, launderers are not required to deal with cash, which is more suspicious to investigators, but uses the virtual assets to move funds across the jurisdictions. Also, these transactions can happen rapidly between senders and recipients in any part of the world without giving much time to AML regulators to notice the transactions.



Fewer Chances of Being Suspected



Transactions of cryptocurrencies are recorded in public domains on the blockchain. Only the individual who carried out the transaction can access their wallet. It is highly encrypted. Therefore, there are fewer chances of linking it to a specific individual or wallet. It reduces the chances of being suspected of money laundering, as the specific transaction by a criminal may get mixed up with genuine transactions over the blockchain.



No Legal Tender

Since cryptocurrencies have no legal tender, they cannot be authorized. Also, anyone can subscribe to it. Since no owner details are maintained, it is easier to launder.

ADDITIONAL INFORMATION & RESOURCES

-  How Money Laundering is messing up the world of cryptocurrency
-  Top 5 methods Criminals use to Launder money



How does Crypto Money Laundering occur?



Gambling and Gaming Websites

Money launderers use illicit cryptocurrencies to buy chips or game currency on gambling websites. Once they are finished with gambling or gaming, they encash the remaining amount. Thus, the illicit cryptocurrency entered the gaming or gambling website is cleaned and converted to cash.

Anonymizing Services

Launderers can hide illicit funds' sources by anonymizing services on crypto exchanges. Anonymizing services break the connection between cryptocurrency transactions. Launderers can also participate in Initial Coin Offering (ICO) – using one type of coin to buy another. Thus, they can disguise the origins of the unlawful money by creating multiple layers.

Tumblers and Mixing Services

Tumblers are mixtures of different digital assets – dirty and clean – from diverse addresses. Once these are blended well, they are redistributed to new addresses or wallets. Once mixed, it is difficult to differentiate the legal and illegal currencies.

Also, by blending the cryptocurrencies, their anonymity increases, making it more challenging for investigators to find the owners. Thus, criminals can save themselves from being suspected and transfer the blended funds to legal businesses or crypto exchanges.

Use of Cryptocurrencies in Terrorism Financing or Paying for Drugs

Many terrorist organizations raise cryptocurrencies through Telegram and Facebook groups. Many intermediaries are involved in transferring such funds to terrorist organizations. Further, money generated from drug trafficking on the internet is converted into cryptocurrencies to disguise the source of such illegal proceeds.

Illegal payments are made in cryptocurrency. Fiat currency is converted to cryptocurrency through a blockchain trading platform. These are later transferred to drug traffickers' accounts.

The payments received in cryptocurrencies are transferred to virtual wallets in different crypto exchanges. Thus, it becomes difficult to trace the origin of funds.

Dark Exchanges

Many unregulated cryptocurrency exchanges operate across the world. They do not conduct any identity checks or KYC of customers or transactions. So, criminals use such exchanges to launder cryptocurrencies. Specifically, launderers use illegal money in fiat currency to open an online account with crypto exchanges.

Money launderers repeatedly transfer illegal currency to multiple accounts or move from one currency to another, thereby developing various layers to cleanse the funds. They sent the cleaned currency to an external cryptocurrency wallet in the last transfer. Alternatively, they convert it into cash using crypto ATMs.

Over-The-Counter (OTC) Brokers

Over-the-counter brokers facilitate transactions between buyers and sellers of cryptocurrencies. They are the intermediaries who get commissions to facilitate transactions. They are involved in converting illegal cryptocurrency to cash or vice versa by charging high commission rates.

Integration Stage

In the integration stage, criminals aim to legitimize illicit cryptocurrency. They have successfully laundered the illegal money but need to show a legal source. In such cases, crypto money launderers create a fake online company that allows crypto currencies as payment methods.

Thus, they transform illegal crypto into legal money by faking the trade transaction. Alternatively, launderers can show the cryptocurrencies as earned towards the sale of a profitable business or an asset appreciation.

Real world Case Studies

Case 1: Silk Road Scandal

Silk road was one of the dark web's largest marketplaces for hosting money laundering activities and illegal drug transaction using crypto currencies, though FBI shut down the Silk Road in 2013.




Their illicit funds were moved through multiple crypto wallets and financial services to cover their origin. Techniques like coin tumbling were used to secure the transaction trail. But with the use of blockchain analysis tools US authorities found the traces of transaction.

Case 2: Binance Investigation

Binance is one of the largest cryptocurrency trading platforms in the world and has been under investigation by the US Justice Department since at least 2018 for failing to meet Anti-Money Laundering (AML) regulations for cryptocurrency.

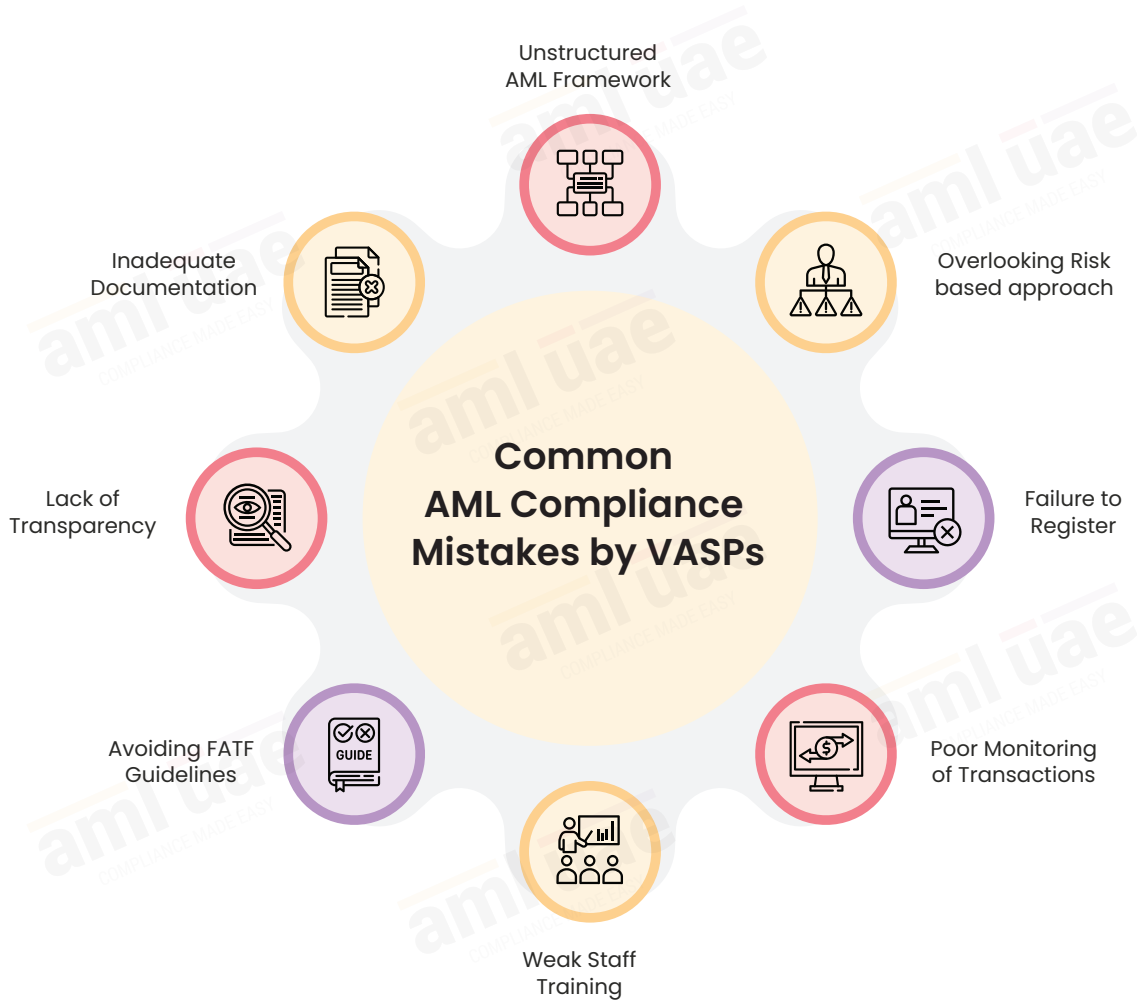
The lack of KYC implementation and insufficient procedures for high-risk entities made it difficult to track transactions effectively, raising concerns about illicit activities.

ADDITIONAL INFORMATION & RESOURCES

-  Stages of Money Laundering
-  What is Integration in Money Laundering?
-  Uncovering the Red Flags of NFT-Related Money Laundering

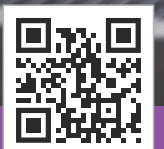
Common AML Compliance Mistakes by VASPs

VASPs often face intense regulatory scrutiny, and principled entities can stumble into compliance pitfalls, here some of the most common mistakes entities make:





What are the Red Flags of Crypto Money Laundering?



Crypto Money Laundering Red flags That VASPs Must Include in Their AML/CFT Policies and Training Programs

When funds are received from a platform that does not have any AML regulations or has been categorized as a jurisdiction with high money laundering risks.

Several high-value transactions suddenly occur in an inactive account or in a new one.

When there are multiple transfers of cryptocurrencies from multiple crypto wallets to one account.

When there are several transactions of purchase of cryptocurrencies by several individuals with the same IP address, followed by several transfers to accounts in another country.

When the crypto sending and receiving transactions are just below the mark of reporting thresholds.

When several credit cards and bank accounts are linked to a single crypto wallet to use it to move funds around.

Connected crypto wallets where the customer profiles do not match.

Continuous occurrence of many high-value transactions in a short time.

When several high-value transactions occur in a regular pattern and stop entirely after a specific period.




When there are cryptocurrency transactions that do not match the profile of a customer.

When there are frequent transactions of fiat conversion to crypto with no logical reasoning.

When many unrelated wallets transfer cryptocurrencies to one common wallet, which immediately converts it to fiat currency.

When transactions occur with digital wallets whose owners are earlier connected to cases of fraud, ransomware, or feature in the sanctions list.

ADDITIONAL INFORMATION & RESOURCES

-  [Uncovering the ML/FT red flags associated with Virtual Assets](#)
-  [Uncovering the Red Flags of NFT-Related Money Laundering](#)
-  [Red Flag Indicators For AML/CFT](#)



How to Combat Crypto Money Laundering?



Yes, there is anonymity in cryptocurrency transactions, which launderers take benefit of. But all the cryptocurrency transactions are documented on a distributed public ledger. These digital records stay permanently. One mistake in the entire money laundering process can help investigators trace the illegitimacy.

One way of protecting cryptocurrencies from money laundering threats is implementing KYC rules. With KYC norms, exchanges could identify the customers and have data about owners of virtual wallets and cryptocurrencies. Registration and licensing of operators in the cryptocurrency market is also a solution that can address the money laundering issue.

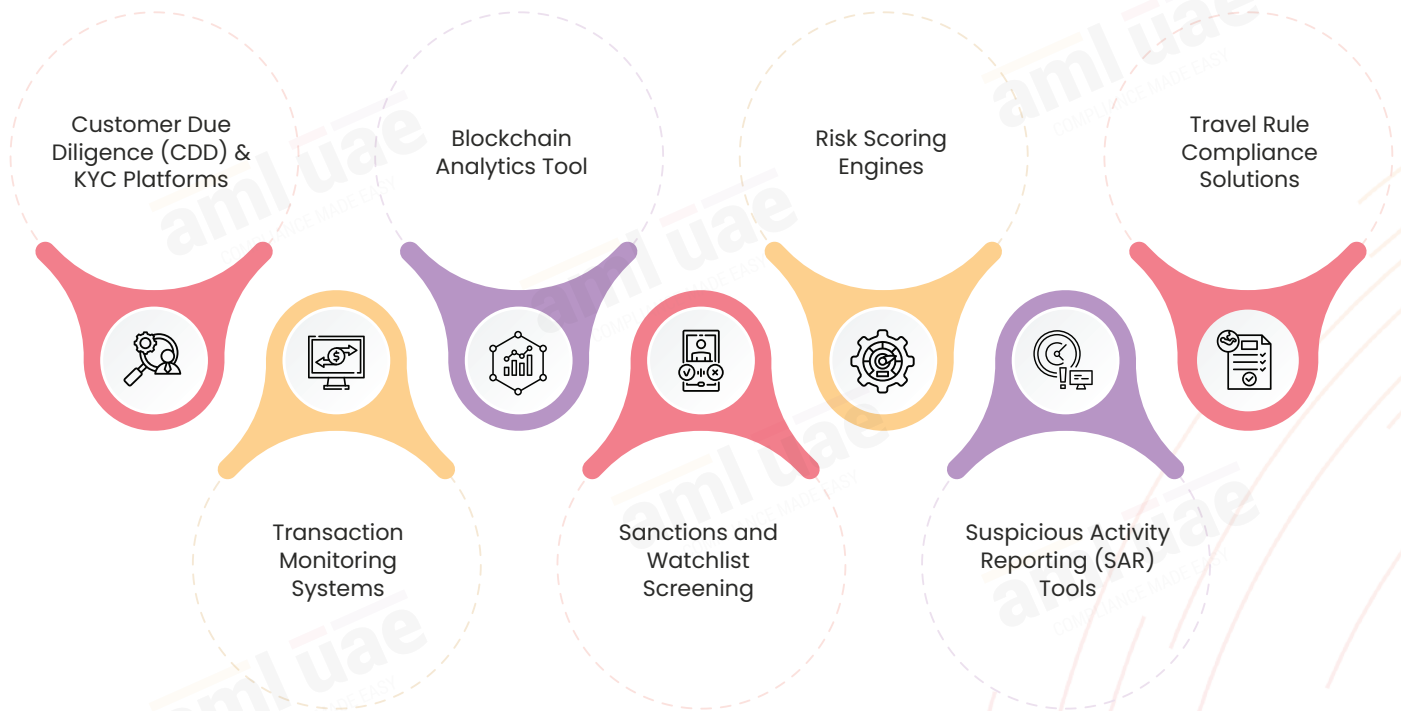
Here is the list of key AML measures the Virtual Asset Service Providers (VASPs) must adopt to identify and combat the crypto money laundering:

- Getting itself registered on the goAML Portal to ensure timely reporting of suspicious activities
- Set up an in-house AML function with a competent AML Compliance Officer and appropriate team to manage the compliance tasks
- Conducting the Enterprise-Wide Risk Assessment to identify the exposure to ML/FT and PF
- Customizing the AML/CFT program in sync with the outcome of EWRA, international best practices and the local AML/CFT regulations to implement the effective combating measures
- Designing and implementing robust Customer Due Diligence program, including Know Your Customer (KYC), customer risk assessment, enhanced due diligence and ongoing monitoring
- Deploying adequate tools and systems to meet the requirements of Know Your Transactions (KYT) and monitor the transactions continuously.
- Compliance with FATF travel rule, including measures to Know Your Counterparty VASPs
- Creating awareness amongst the team with adequate AML training
- Adopting mechanism to identify the red flags and timely report the suspicious activities and transactions on the goAML Portal

- Implement the Targeted Financial Sanctions (TFS) program to prohibit any transaction with designated people
- Ensuring periodic AML audit of the entire function

AML Tools that VASPs Can Leverage

Virtual Asset Service Providers (VASPs) use a range of Anti Money Laundering (AML) tools to stay compliant with regulations and detect suspicious activity in the crypto business, some of the mostly used tools include:





FATF Recommendations Concerning VASPs



FATF has issued updated recommendations to assist countries in combating misuse of virtual assets and services. The lack of implementation of regulations creates loopholes that criminals and terrorists can take advantage of entities. key directives include:

- Mandatory KYC and customer identity verification by VASPs.

- Continuous transaction monitoring for high-risk customer.

- Government registration/licencing of VASPs to ensure that they comply with AML/CFT regulations.

- The Travel Rule requires accurate information on both parties to be shared with beneficiary VASPs during cross-border virtual asset transfers.

- To improve transparency and traceability, key customer information should be transferred alongside the digital assets.

- To prevent the facilitation of illicit activities, it is essential to perform comprehensive CDD, continuous monitoring transactions and adhering strictly to applicable regulations.

- Periodic review and updates of customer information are necessary as risk profiles change.

- Offshore VASPs being addressed through stronger international cooperation to prevent regulatory loopholes.







- Stablecoins being closely monitored as they become primary channel for illicit activity.

- DeFi platform, despite being decentralized, need to follow appropriate rules and regulations to ensure security and transparency.

- Enforcement against noncompliance with penalties ranging from blacklisting to criminal liability.

- These measures emphasize that compliances is not just checklist but a critical safeguard against legal and financial exposure.

ADDITIONAL INFORMATION & RESOURCES

-  [AML Policy Template for the VASP in UAE](#)
-  [Exploring unusual transaction trends for VASPs under UAE AML Regulations](#)
-  [Sanctions Compliance by VASPs in UAE: Safeguarding the Virtual Asset segment against financial crimes](#)
-  [AML Governance for VASPs in the UAE: Building trust and strengthening compliance](#)
-  [The Vital Role of an AML Compliance Officer in Safeguarding VASPs in the UAE](#)
-  [What is NFT money laundering and how to combat it?](#)



FAQs on Crypto, VASPs and Its Regulating Authorities



Q. What are virtual assets examples?

Ans. Virtual assets include digital art, text, videos, in-game items, images, music, etc. represented as non-fungible tokens, cryptocurrencies, and virtual real estate.

Q. Are virtual assets also known as cryptocurrency?

Ans. A cryptocurrency is a type of virtual asset. But not all virtual assets are cryptocurrencies.

Q. Who regulates the crypto, NFT, and virtual assets onshore/mainland companies in UAE?

Ans. The VASPs licensed and operating in Emirates of Dubai (other than DIFC) are regulated by Virtual Assets Regulatory Authority (VARA). While the VASP in DIFC are subject to supervision of Dubai Financial Services Authority and the ones operating in ADGM are regulated by ADGM's Financial Services Regulatory Authority.

All other VASPs are governed by UAE's Securities and Commodities Authority (SCA).

Q. What AML compliance requirements do Crypto companies, NFT, and other Virtual Asset Service Providers in UAE have to follow?

Ans. Following are the Anti-Money Laundering (AML) compliance requirements that Crypto Companies, NFT, and other Virtual Asset Service Providers (VASPs) in UAE have to follow:

- VASPs have to register on the goAML Portal
- VASPs are required to appoint the AML Compliance Officer to manage the AML/CFT program.
- Virtual Asset Service Providers have to conduct Business Risk Assessment (BRA)
- VASPs have to prepare their AML Policy and Procedures Manual
- VASPs need to conduct KYC, Screening, Risk Assessment of customers, suppliers, and third-parties
- Crypto Companies and other virtual asset service providers have to file certain AML related reports on the goAML Portal
- VASPs have to provide Anti-Money Laundering training to employees and senior management

Q. Who regulates crypto and other virtual assets companies housed in Abu Dhabi Global Market (ADGM)?

Ans. The Abu Dhabi Global Market (ADGM) based crypto and other virtual asset companies are supervised by the Financial Services Regulatory Authority (FSRA).

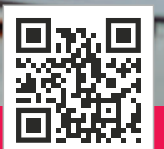
Q. What are the Anti-Money Laundering (AML) laws and regulations applicable to Virtual Asset Service Providers (VASPs) in UAE?

Ans. Primarily, the crypto, NFT, and other virtual assets companies in UAE have to adhere to the requirements of the following anti-money laundering (AML) laws and regulations:

- The Federal Decree-Law No. (20) of 2018
- Cabinet Decision No. (10) of 2019
- Cabinet Decision No. (74) of 2020
- AML Guidelines issued by the respective AML governing authority such as Compliance and Risk Management Rulebook issued by VARA



How can AML UAE assist you in AML Compliance?



AML UAE is a leading provider of AML/CFT consulting services.

We help our clients develop an effective AML compliance framework for their operations.

With thorough understanding of the virtual asset ecosystem and regulations, we help VASPs conduct the Enterprise-Wide Risk Assessment (EWRA) and define the necessary controls to safeguard the crypto industry.

We help clients with ML/FT policy, procedure, risk assessment, determination of red flags, managed KYC and CDD services, regulatory reporting, and creation of transaction monitoring rules aligned with your business profile.

We understand the significance of transaction monitoring and compliance with FATF travel rule by a VASP.

Accordingly, we can also assist you with selecting effective transaction monitoring software and implementing it with our AML experts' support. We made compliance easy and cost effective.



About AML UAE



AML Compliance Simplified!

AML UAE is an anti-money laundering (AML) consulting firm operating and supporting Businesses across the UAE with decades of experience.

We have expertise in providing various AML services to DNFBPs like Real Estate Agents, Accountants and Auditors, Dealers in Precious Metals and Stones, Trust and Company Service Providers, and Lawyers. We also provide AML consultancy services to Virtual Asset Service Providers.

We are equipped to help you with registering on the goAML portal. We conduct Enterprise-Wide Risk Assessments and align your AML/CFT policies and procedures in line with it. We provide you with various templates for carrying out KYC, Screening, and Risk Assessment of your customers. We help you with submitting various reports like SAR, STR, FFR, PNMR, HRC, HRCA, DPMSR, REAR, etc. We ensure that your employees are well-trained from an AML perspective.

AML UAE is your go-to partner that can handle all your compliance-related requirements. Once we come into the picture, AML compliance is ensured. With that, you can continue to stay a highly reputed business, actively striving to counter money laundering and terrorist financing



Service Matrix

Service	Common Drivers							Value Proposition
	Ensure legal compliance	Save time and costs	Need expert support	Automate compliance processes	Implement best practices	Crisis management	Change AML/CFT consultant	
goAML Registration	✓		✓					Streamlines the process of registering with the UAE FIU goAML portal. Ensures compliance and reduces administrative burden.
Enterprise-Wide Risk Assessment	✓	✓	✓		✓		✓	Identifies risk factors, gross risk, controls deployed and their effectiveness, residual risk, and need for additional controls.
AML/CFT Policy Drafting	✓	✓	✓		✓		✓	Provides tailored AML/CFT policy frameworks that are up-to-date with current laws, enhancing regulatory compliance.
In-house Compliance Department Set-up	✓		✓		✓		✓	Establishes a robust internal compliance structure, helps recruit the right resources and ensures ongoing compliance efficiency.
KYC Managed Services	✓	✓	✓		✓	✓		Outsourced KYC processes that speed up customer onboarding and maintain high compliance standards.
Ongoing AML/CFT Consulting	✓	✓	✓	✓	✓	✓	✓	Continuous expert advice tailored to address specific challenges, enhancing overall compliance strategies.
AML/CFT Health Check	✓		✓		✓	✓	✓	Conducts comprehensive reviews and assessments to pinpoint vulnerabilities and recommend improvements.
AML Training	✓	✓	✓		✓		✓	Offers comprehensive training programs that enhance the compliance skills of employees at all levels.
AML Software Selection	✓	✓	✓	✓	✓			Helps choose the best AML software that fits the company's needs, improving efficiency and cost-effectiveness.
Screening Software Validation	✓		✓	✓	✓			Tests and validates screening tools to ensure they meet regulatory requirements and operational needs.
Regulatory Reporting	✓	✓	✓		✓		✓	Streamlines the process of creating and submitting SAR, STR, PNMR, FFR, DPMSR, REAR, HRC, and HRCA reports accurately and on time.

Our Team



Pathik Shah 

FOUNDER

CAMS, FCA, CISA, CS, DISA (ICAI), FAFP (ICAI)

Pathik is a Chartered Accountant with over 26 years of experience in governance, risk, and compliance. He helps companies with end-to-end AML compliance services, from conducting Enterprise-Wide Risk Assessments to implementing robust AML compliance frameworks. He has played a pivotal role as a functional expert in developing and implementing RegTech solutions for streamlined compliance.



Jyoti Maheshwari 

PARTNER

CAMS, ACA

Jyoti is a Chartered Accountant and Certified Anti-Money Laundering Specialist (CAMS), having around 8 years of hands-on experience in regulatory compliance, legal advisory, policy-making, tax consultation, and technology project implementation. Jyoti holds experience with Anti-Money Laundering regulations prevalent across various countries. She helps companies with risk assessment, designing and deploying adequate mitigation measures, and implementing the best international practices to combat money laundering and other financial crimes.

Our Team



Dipali Vora 

PARTNER
CAMS, ACS

Dipali is an Associate member of ICSI and a Certified Anti-Money Laundering Specialist (CAMS). She has an overall experience of 8 years in the compliance domain, including Anti-Money Laundering, due diligence, secretarial audit, and managing scrutiniser functions. She currently assists clients by advising and helping them navigate through all the legal and regulatory challenges of Anti-Money Laundering Law. She helps companies to develop, implement, and maintain effective AML/CFT and sanctions programs.



Purva Buch 

Senior Consultant
CAMS, LLB

Purva is a Certified Anti-Money Laundering Specialist (CAMS) and a Lawyer with 5+ years of experience. She has substantial knowledge of Anti-Money Laundering Laws, Rules, Regulations, and AML Compliance Processes. Purva has been instrumental in drafting RegTech processes, corporate policymaking, and fulfilling various legal research and drafting requirements arising from AML laws and regulatory technology.

AML Verse

<p>aml singapore</p> <p>AML/CFT compliance ensured with precision and expertise. Safeguarding your business at every step</p> <p>amsingapore.com</p>	<p>AML Consultants.UK</p> <p>UK's first choice for AML, CFT, and CPF compliance and consulting.</p> <p>amlconsultants.uk</p>	<p>aml india</p> <p>Enjoy peace of mind as AML/CFT compliance is ensured with professional guidance and proven solutions</p> <p>amlindia.in</p>	<p>aml australia</p> <p>Protecting Australia's financial landscape with trusted AML compliance solutions</p> <p>amlaustralia.com</p>
<p>AML Consultants.us</p> <p>Your trusted partner in simplifying AML compliance, ensuring regulatory adherence and protecting your business.</p> <p>amlconsultants.us</p>	<p>aml ksa</p> <p>At the core of our business is ensuring AML/CFT compliance for yours.</p> <p>amlksa.com</p>	<p>aml bahrain</p> <p>Our priority is your peace of mind – ensuring AML/CFT compliance is how we deliver it</p> <p>amlbahrain.com</p>	<p>aml muscat</p> <p>Timely service, flawless compliance, and peace of mind – your AML/CFT partner you can trust</p> <p>amlmuscat.com</p>
<p>PRO AML</p> <p>Guiding budding AML/CFT professionals to ignite their potential and excel in compliance leadership</p> <p>proamltraining.com</p>	<p>aml job</p> <p>Connecting AML talent with global opportunities for financial integrity</p> <p>recruit.amljob.com</p>	<p>aml faqs</p> <p>Ask, Answer, Comply: Your one-stop hub for AML/CFT compliance knowledge</p> <p>amlfaqs.com</p>	<p>Technovisors</p> <p>IT Consultants & Digital Marketing Consultants to help you focus on your business</p> <p>technovisors.com</p>
<p>N NIYEAHMA</p> <p>We help regulated entities with End-to-End AML Compliance</p> <p>niyehma.com</p>			

aml uae
COMPLIANCE MADE EASY



Follow us on



 www.amluae.com  info@amluae.com