VALOORES

The FATF QUANTUM Leap Transforming Compliance Standards The VALOORES Blueprint Crafting Compliance & Investigation Excellence

In today's rapidly evolving financial landscape, cryptocurrencies and digital assets continue to reshape markets, driving unprecedented transformation across industries and stakeholder ecosystems. As the financial services sector experiences this technological paradigm shift, regulatory frameworks are progressively adapting, with jurisdictions worldwide implementing comprehensive oversight mechanisms aligned with FATF's strategic guidance on risk mitigation. VALOORES, positioned at the intersection of innovation and compliance, delivers enterprise-grade solutions through its Crypto Management System (VCMS), offering institutional stakeholders a sophisticated platform that ensures robust asset protection and regulatory alignment while enabling organizations to navigate market volatility with enhanced operational confidence.

By seamlessly integrating cutting-edge risk mitigation protocols and robust security measures, VCMS not only shields against emerging threats but also pioneers a new era in digital asset management.

Table of Contents

Introduction

In an era of unprecedented digital transformation and financial interconnectivity, the integration of cryptocurrencies and digital assets into the global financial infrastructure presents both strategic opportunities and complex regulatory imperatives. Financial institutions, regulatory authorities, and Virtual Asset Service Providers (VASPs) face mounting pressure to implement robust Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) frameworks that meet evolving international standards.

The Financial Action Task Force (FATF), as the preeminent global authority on financial compliance, continues to shape the regulatory landscape through comprehensive governance frameworks. With a legacy spanning three decades, FATF's evolving mandate has established industry-leading standards for combating financial crime, adapting its protocols to address the sophisticated challenges presented by the digital asset ecosystem. This dynamic regulatory environment demands innovative solutions that can adapt to emerging threats while maintaining operational efficiency.

VALOORES delivers enterprise-grade solutions designed to meet FATF's complex compliance requirements, enabling organizations to achieve operational excellence while maintaining the highest standards of security and transparency. Through our integrated suite of solutions—VCMS, VCMS, and VFDS—we empower stakeholders across financial services, virtual asset operations, and law enforcement sectors to enhance their compliance frameworks, strengthen resilience against financial threats, and establish sustainable trust through systematically compliant operations. Our comprehensive approach ensures institutions remain at the forefront of regulatory compliance while optimizing their operational capabilities in an increasingly complex financial landscape.

Chapter 1: VCMS At the Forefront of FATF Compliance In the Realm of Virtual Assets

In response to the growth of digital assets, the FATF updated its recommendations in October 2018 to include financial activities related to virtual assets. This crucial expansion provided specific definitions for "virtual assets" (VAs) and "virtual asset service providers" (VASPs), establishing a framework to address the AML and CFT challenges unique to this sector.

A. Definition of Virtual Assets and VASPs

Virtual assets are defined as digital representations of value that can be traded or transferred electronically and used for payment or investment. These assets do not cover digital forms of fiat currencies, securities, or other financial assets addressed by existing FATF standards. A "virtual asset service provider" encompasses entities facilitating transactions involving virtual assets, such as exchanges, transfers, safekeeping, and financial services related to virtual asset offerings. These cover the following VASPs categories:

1. Exchange between virtual assets and fiat currencies;
2. Exchange between one or more forms of virtual assets;
3. Transfer of virtual assets; and
4. Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets;
5. participation in and provision of financial services related to an issuer’s offer and/or sale of a virtual asset.

B. The Risk-Based Approach (RBA) for VAs and VASPs

In 2019, FATF issued an Interpretive Note to Recommendation 15, focusing on a risk-based approach (RBA) for virtual assets. This approach requires VASPs to assess and address AML/CFT risks according to the unique nature of virtual assets. VASPs must undergo robust monitoring, licensing, and preventive procedures, including customer due diligence, recordkeeping, and suspicious activity reporting.

C. Ongoing Guidance and Compliance Reviews

FATF's continuous updates, including guidance on digital identity verification (March 2020), and the release of Red Flag Indicators for VAs (September 2020), have underscored the organization's commitment to adaptive regulatory standards. FATF’s two-year review of revised VA standards in July 2021 reinforced the need for clear protocols for assessing, understanding, and mitigating risks in the virtual asset space.

D. Country-Level Compliance Requirements

The FATF mandates that countries evaluate ML/TF risks within their jurisdictions and ensure that VASPs actively implement measures proportional to these risks. Competent authorities must work with VASPs to evaluate services, products, customer profiles, and geographical influences. This alignment ensures that VASPs effectively identify and mitigate risks and promotes consistent adherence to global standards.

Through these comprehensive guidelines, the FATF has solidified its position in overseeing the integrity of digital asset ecosystems. At VALOORES, we are dedicated to supporting organizations in their journey toward FATF compliance, offering tools that enhance the resilience and security of the financial network across traditional and virtual domains. Our mission is to bridge the gap between compliance and operational efficiency, ensuring our clients are equipped to thrive in an increasingly regulated digital landscape.

E. The FATF Travel Rule

The FATF Travel Rule, part of Recommendation 15 on New Technologies, mandates that Virtual Asset Service Providers (VASPs) gather and share specific identifying information on the originator and beneficiary of virtual asset transactions above a certain threshold. This requirement mirrors the standards applied to wire transfers in traditional finance, aiming to increase transparency and prevent misuse of virtual assets in money laundering and terrorist financing. VASPs must collect, verify, and securely transmit essential information such as the name, account number, and geographical address or national ID number of both the sender and receiver. Additionally, VASPs are required to ensure secure data handling to protect customer information and maintain regulatory compliance across jurisdictions. By adhering to the Travel Rule, VASPs support global AML/CFT objectives and contribute to a safer, more transparent financial environment.

F. Beyond Recommendation 15

1. FATF Recommendations for VASPs

VCMS ensures that VASPs comply with FATF’s comprehensive Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) standards by supporting key recommendations relevant to private sector compliance. Through automated tools, advanced data analytics, and machine learning, VCMS addresses the following FATF standards:

Recommendation 10: Customer Due Diligence (CDD)

VCMS strengthens Customer Due Diligence (CDD) practices by automating the verification and ongoing monitoring of customer information, ensuring compliance with AML/CFT standards. Key data such as customer identity, transaction history, risk level, and beneficial ownership is rigorously assessed to enable VASPs and financial institutions to identify and monitor customer risks continuously, particularly for higher-risk clients.

Recommendation 12: Politically Exposed Persons (PEPs)

VCMS includes a dedicated module for identifying and monitoring politically exposed persons (PEPs), including domestic, foreign, and international individuals with prominent public functions. Real-time monitoring and periodic screenings ensure heightened due diligence, enabling VASPs to address risk effectively and in accordance with FATF's requirements.

Recommendation 16: Wire Transfers

VCMS aligns with FATF's standards on transparency for wire transfers, ensuring VASPs trace the origin and beneficiaries of transactions, including crypto-to-crypto and crypto-to-fiat transfers.

Recommendation 20: Suspicious Transaction Reporting

By integrating advanced analytics and anomaly detection, VCMS flags unusual or high-risk transactions that may indicate potential money laundering or terrorist financing activities. The system automatically generates reports for suspicious transactions, facilitating timely investigation and reporting to Financial Intelligence Units (FIUs) as required by FATF guidelines.

Recommendation 24: Transparency and Beneficial Ownership of Legal Persons

VCMS allows VASPs to track beneficial ownership details, providing transparency across ownership chains. This enables institutions to comply with FATF's standards on identifying ultimate beneficial owners, especially for transactions involving complex ownership structures, ensuring accountability and fostering trust within the virtual asset sector.

Recommendation 35: International Cooperation

VCMS is designed to support cross-border cooperation by facilitating secure data sharing among VASPs, financial institutions, and relevant authorities. This compatibility with international AML/CFT standards enables seamless collaboration across jurisdictions, reinforcing FATF's call for global cooperation in the fight against financial crime.

2. FATF Recommendations for Law Enforcement Agencies

VCMS is equally equipped to empower public sector entities such as law enforcement and regulatory bodies in conducting investigations and enforcing compliance within the digital asset ecosystem. It offers investigative capabilities aligned with FATF recommendations, ensuring that agencies can tackle illicit financial activities effectively:

Recommendation 30: Responsibilities of Law Enforcement and Investigative Authorities

Through VCMS, law enforcement agencies have access to tools that support their responsibility to investigate money laundering and terrorist financing within the AML/CFT framework.

Recommendation 31: Powers of Law Enforcement and Investigative Authorities

VCMS enables law enforcement to leverage advanced investigative techniques necessary for financial crime investigations. These include undercover operations, intercepting communications, controlled deliveries, and access to critical data on account holders.

Recommendation 32: Cash Couriers and Virtual Assets

VCMS provides mechanisms to monitor large cryptocurrency movements that may bypass traditional financial systems, addressing FATF’s focus on detecting illicit cross-border transfers. This feature assists law enforcement in jurisdictions with significant informal value transfer activities, ensuring oversight over cross-border currency transport and cryptocurrency transfers.

Why VCMS?

By aligning with FATF standards, VCMS provides a comprehensive compliance and investigation solution for both private VASPs and public sector law enforcement. Its design addresses key FATF recommendations that foster a transparent, secure, and accountable digital asset ecosystem. Through VCMS, VALOORES equips entities with the tools needed to meet evolving AML/CFT obligations, mitigate financial crime risks, and support international cooperation across the virtual asset landscape.

Chapter 2: VCMS Compliance Capabilities

A. Crypto Digital KYC Solution implementation

1. VCMS: A Comprehensive Digital KYC Solution for Cryptocurrency Compliance

VALOORES' Virtual Compliance Management System (VCMS) is designed to support government agencies, financial institutions, and regulatory bodies in upholding FATF-compliant cryptocurrency KYC protocols. The VCMS platform uses advanced biometrics technology to verify and authenticate user identities, thereby safeguarding virtual asset transactions from potential risks. VCMS integrates a robust suite of KYC features to ensure accurate identity verification, streamline due diligence, and enhance the overall compliance process for virtual assets

2. Core Features of VCMS Digital KYC and Identity Verification

Advanced Biometric and Document Verification

VCMS utilizes state-of-the-art identity verification methods to ensure secure, reliable identification. This process helps verify user authenticity seamlessly while enhancing compliance with global standards.

Geospatial Verification

VCMS incorporates location-based checks, enabling enhanced user verification and adding a powerful layer of fraud protection to safeguard transactions.

Cross-Border Compliance

Aligned with FATF's Travel Rule, VCMS supports international compliance requirements, making cross-border transactions transparent and secure.

3. Data Collection and Verification Points

Identity and Contact Information

VCMS collects essential identifying information such as user details, residence data, and contact channels to establish a solid identity profile for each individual, supporting secure onboarding and account management.

Employment & Financial Information

Key data related to a user's professional background and financial standing provides insights into transaction legitimacy, ensuring compliance with industry standards.

Account Activity Insights

VCMS gathers basic account and transaction details, including identifiers that link users to specific accounts, to foster transparency and traceability in digital asset interactions.

Identity Confirmation

VCMS employs verification measures to confirm identity details against official records and uses biometric validation tools to enhance user authenticity, particularly for higher-risk accounts. Geographic data is also assessed to support location-based verification.

4. Automated Trigger Points for Enhanced KYC Monitoring

High-Value Transactions

VCMS automatically initiates enhanced monitoring for transactions above a defined threshold to mitigate risks associated with large transfers.

Geographic Risk Indicators

Accounts accessed from regions associated with heightened risk are subject to additional compliance checks, helping to reinforce secure operations.

Account Behavior and Anomaly Detection

VCMS continuously monitors for unusual activity patterns, including multiple or frequent account adjustments, ensuring a responsive and proactive approach to user risk.

B. Wallet Name Matching System (WNMS)

Our matching system is engineered to simultaneously match names and wallets, constituting a multitask matching system that operates on intricate and advanced criteria. This capability enables our solution to adopt a defensive approach to money laundering by utilizing lists that can be implemented within the system to detect matching names or wallets, while also adhering to all international standards regarding crypto compliance. For example UN 1267 list which refers to the United Nations Security Council (UNSC) Consolidated List, This list is maintained by the United Nations Security and it aims to impose sanctions, such as asset freezes and travel bans, on those deemed to be involved in terrorist activities.

Another example would be the national list 1373. It established a framework for combating terrorism and called upon all UN member states to take various measures to prevent and suppress terrorist activities.

Any list or sources of data can be integrated into the solution to enhance the ability to identify all Crypto users who are considered suspicious.

C. Crypto Risk Based Approach (CRBA)

Incorporating cryptocurrency into the Basic Risk Matrix and Case Relative Risk adds an extra layer of complexity and sophistication to the RBA risk-based approach in KYC.

1. **Cryptocurrency Transaction Analysis in the Risk Matrix:**

- In the detailed Risk Matrix, one can integrate the analysis of cryptocurrency transactions associated with an individual or entity. Cryptocurrency transactions often present unique challenges and opportunities for risk assessment. Unusual patterns, high-frequency transactions, or connections to known illicit activities in the crypto space can significantly impact the calculated risk.

- Admin users might have the capability to override the risk based on specific cryptocurrency-related findings. For instance, if an individual is involved in multiple transactions flagged for potential money laundering or fraud, the admin user could adjust the risk level accordingly.

- Clicking on the risk lookup could reveal not only traditional risk factors but also detailed insights into cryptocurrency-related risks. This might include involvement in dark web transactions, association with flagged wallet addresses, or engagement in activities linked to cryptocurrency-based scams.

2. **Cryptocurrency Tracking in Case Relative Risk:**

- The VCMS Tool can extend its capabilities by incorporating cryptocurrency-related information to identify potential risks. Individuals who might seem harmless based on conventional indicators could be flagged if their cryptocurrency transactions align with suspicious patterns.

- The VCMS could raise a relative risk alert if someone is found to have engaged in cryptocurrency transactions linked to known criminal activities or has received funds from a wallet associated with illicit practices. This approach allows for a more nuanced and targeted identification of risks, especially when dealing with cases involving cryptocurrency-related crimes.

By integrating cryptocurrency analysis into the risk matrices, KYC processes become more comprehensive and adaptive to the evolving landscape of financial transactions, providing a more effective means of identifying and mitigating potential risks associated with individuals or entities.

D. Crypto Rules and Transaction Monitoring

Our solution operates on a framework of dynamic rules specifically customized for cryptocurrency transactions. These rules are meticulously implemented across one or more blockchain ledger databases, forming the backbone of our system's capability to identify suspicious activity. When triggered, these rules generate alerts that are meticulously analyzed, taking into account transaction specifics and the historical data associated with the relevant wallet. This meticulous analysis ensures that any potential risks or illicit behavior are thoroughly investigated, allowing for swift and effective response measures to be taken.

1. Implementing the Travel rule based on FATF rec. 15

In the context of cryptocurrencies, the Travel Rule requires VASPs to exchange specific customer information (such as name, address, and account number) for transactions exceeding a certain threshold. This information is transmitted securely between the originating VASP (the sender's provider) and the beneficiary VASP (the recipient's provider) to facilitate compliance with AML/CFT regulations.

Based on Recommendation 15,the Travel Rule aims to enhance transparency and traceability in cryptocurrency transactions, thereby mitigating the risk of illicit activities such as money laundering and terrorist financing within the virtual asset space.

2. Transaction Monitoring Location Base

Many financial institutions continue to rely on IP addresses to verify a user's location, even though this method is vulnerable to spoofing and is not very effective. However, by implementing VCMS and VCMS, which include a real-time and historical risk engine and patterns of behavior in correlation with geospatial data, suspicious activities and high risk acts can be detected by identifying the country of residence, country of work, nationality, other nationality, secondary resident country, country of registration, country of incorporation, parent registration company and others.

3. Same Transaction Amount Monitoring

Sometimes, suspicious or illegal activities can go unnoticed when a certain amount of money is transferred periodically, appearing as a normal pattern. However, with VCMS, such transaction processes can be compared against several parameters, such as the income and social class of the sender based on our solution's classification, as well as the recipient's identity and location, in order to identify potential fraudulent or illegal activity.

Exchange Locations & Amounts Records

The increasing use of faster payment methods and digital acceleration has created an environment that fraudsters and cybercriminals can exploit. For instance, they may attempt to make multiple transactions from a single account located in different, distant locations within a short period of time. However, VCMS utilizes the ledger database to identify patterns and track changes in customer behavior by examining the scope of generated alerts over a specific period. This solution can also help locate the accurate site of the account owner and stop any suspicious activity as soon as it is detected.

Chapter 3: VCMS role in Crypto investigations

A. Location Intelligence

In today's world, billions of devices are connected to the Internet of Things, granting executives and decision-makers unparalleled access to business data, including a plethora of geospatial information. Geo-Smart Location enables the visualization and analysis of vast volumes of data in a location-specific context, empowering holistic planning, prediction, and problem-solving. By viewing all pertinent data in the context of location, whether on a smart map, app, or dashboard, unique insights can be gleaned.

Geospatial data combines location information (usually coordinates on the earth), and often also temporal information, the time or life span at which the location and attributes exist. There are many benefits to using geospatial data for cyber security. With geospatial data, cyber threat data can be captured, including, for example, the location of attacks, the number of attacks, the proportion, dates, types, and various other factors.

B. VCMS Value Proposition

1. Visibility

VCMS provides unparalleled "Global Visibility" by offering data insights beyond borders. The software manages a vast amount of data.

2. Data Correlation with Multiple Data Sources

A key feature of VCMS is "Data Correlation with Multiple Data Sources," integrating telecom data (CDR & SDR), tracking device data and other consolidation sources. This comprehensive approach allows investigators to establish connections and patterns across diverse datasets, facilitating a holistic understanding of criminal activities.

3. Offline System

VCMS ensures security and accessibility with its "Offline System," operating as a standalone server without the need for an internet connection. This feature is crucial for sensitive investigations, allowing law enforcement to maintain control over access to critical crime and geospatial data.

4. Friendly Graphical User Interface

VCMS prioritizes user experience with a "Friendly Graphical User Interface" that synchronizes different platforms among agencies. The software offers different data modules in one suite, eliminating the need for technical skills. This user-friendly design promotes efficient collaboration and information sharing among investigators, ensuring that agencies can seamlessly work together to analyze geospatial data and combat various crime types.

5. Technology, Big Data, and AI

VCMS integrates cutting-edge "technology, big data, and AI" handling both structured and unstructured data. The software efficiently ingests large amounts of data in measurable time, executing queries and scenarios in seconds.

6. Navigating in Time

VCMS introduces the innovative feature of "Navigating in Time," facilitating backward and forward investigation. Investigators can understand the past, analyze the present, and predict the future. This temporal navigation enhances the software's capabilities to provide a dynamic and comprehensive view of criminal activities over time, empowering investigators to make informed decisions based on historical context and future trends.

C. VCMS’s Role in combating Crimes Using Cryptocurrencies

Enhancing Cryptocurrency Crime Detection with VCMS Geospatial Capabilities:

1. Tracking Crypto Wallet Devices Using Geospatial Technology

VCMS empowers law enforcement to track devices associated with crypto wallets through device IDs stored in its Digital Know Your Customer (DKYC) database. DKYC contains detailed personal and technical information on wallet owners, enabling real-time monitoring of device activities and uncovering links with individuals flagged as high-risk or criminally affiliated.

2. Dynamic Knowledge Graph for Tracking Crypto Transactions

VCMS employs a dynamic knowledge graph that monitors cryptocurrency transactions across blockchain ledgers. This graph visually maps relationships and flows of crypto assets, aiding in the detection of funds movement across wallets and exchanges, including cross-chain transfers. By correlating wallet addresses with individuals or entities using DKYC, VCMS provides law enforcement with enhanced tracking and transparency of crypto transactions.

3. Identifying Wallet Owners through Geospatial Data Correlation

Using AI, VCMS links wallet addresses to owners in specific regions by correlating geospatial data with online ledger information. This includes automatically linking device IDs with wallet addresses, which is saved in the KYC database, enhancing identification accuracy. The AI engine further analyzes user behavior, activities, and connections within the crypto ecosystem, supporting law enforcement's efforts to monitor suspicious activity.

4. Financial Crime Links and Points of Interest (POI) Circles

By combining machine learning with Geo-Smart analytics, VCMS establishes a network of individuals and financial associations. This spatial analysis allows law enforcement to visualize connections between transactions, individuals, and POIs, providing context and rapidly identifying new relationships. This real-time analysis supports quick, proactive decision-making around suspicious activity.

5. Location-Based Authentication for Enhanced Security

VCMS uses location-based authentication to verify transaction origin by analyzing the physical location against pre-authorized areas. If a transaction occurs outside expected zones, the system triggers security responses or alerts, helping prevent unauthorized access or fraud. This geospatial check adds a robust layer of defense by scrutinizing real-time data for transaction integrity.

6. Risk Analysis and Anomaly Detection through Geospatial Data

By integrating geospatial data with security algorithms, VCMS discerns regular from irregular transaction patterns. Anomalies, like sudden changes in transaction location, prompt investigations or security responses to address potential fraud. This proactive detection capability allows financial institutions to react swiftly to emerging threats, minimizing security risks.

Conclusion

The rapid evolution of cryptocurrencies has redefined financial systems worldwide, creating unique opportunities while intensifying the need for robust, regulatory-aligned solutions. This analysis underscores the urgent necessity for secure, compliant integration of cryptocurrencies within the global financial framework—an objective that aligns seamlessly with FATF standards.

Through the deployment of advanced tools such as Crypto Digital KYC, Wallet Network Monitoring Systems (WNMS), Continuous Risk-Based Authentication (CRBA), and sophisticated transaction monitoring, VCMS supports institutions and law enforcement in their commitment to global compliance standards. By enabling a thorough, secure, and scalable approach to crypto transactions, VCMS offers a compliance-driven infrastructure capable of adapting to the evolving demands of FATF guidelines, ultimately enhancing transparency, mitigating financial crime risks, and fortifying the resilience of the global financial ecosystem.

The role of VCMS in digital asset investigations stands as a testament to the power of innovative technology in upholding accountability and trust in the crypto sphere. As the industry continues to expand, the need for solutions that balance technological advancement with regulatory rigor remains paramount. VCMS is positioned to lead this effort, ensuring that as the financial ecosystem adapts to modern demands, it does so with an unwavering commitment to security, compliance, and sustainable growth.

ABOUT VALOORES

Careers
Press Release
Quotes

CONTACT US

Access Dashboards
Office Locations
E-mail

LINES OF BUSINESS

in'Banking
in'Technology
in'Insurance
in'Healthcare
in'Government
in'Analytics
in'Academy
in'Retail
in'Multimedia
Webinars

SERVICES

in'AML
in'Regulatory
in'Merch
in'IRFP
in'AI/BI
in'KYC
in'Fraud Management
in'Via
in'Consultancy
in'Profit
in'Campaign
in'IFRS9