

The Age of Regulation for Crypto Asset Service Providers: Technical Compliance Strategies

➤ I. INTRODUCTION AND REGULATORY REQUIREMENTS

1.1. The Financial Institution Status of Cryptocurrency Exchanges: Transition from Technology Company to Obligor

Historically, crypto asset exchanges have generally positioned themselves as "technology infrastructure providers," distancing themselves from the strict obligations of traditional financial institutions. This approach has supported the sector's innovative and rapid growth dynamics. However, because these platforms facilitate trading in the markets, influence price formation, and, most importantly, hold user funds within their own structures, the sustainability of this restrictive definition has been questioned by national and international authorities. The fact that an institution controls user assets beyond providing technological infrastructure means that it cannot avoid financial regulations.

This legal debate has resulted in a critical transformation in the Republic of Turkey. With the amendment to the Measures Regulation published in the Official Gazette dated December 25, 2024, Crypto Asset Service Providers (CASP) have been officially recognized as financial institutions. This change in legal status has placed CASS under similar strict obligations as banks and brokerage firms under Law No. 5549 on the Prevention of Money Laundering and the related Compliance Program Regulation. CASP are now responsible for fulfilling fundamental regulatory objectives such as investor protection, financial stability, and managing AML/CFT (Anti-Money Laundering/Countering the Financing of Terrorism) risks.

1.2. Analysis of Legal and Financial Risks: The Exponentially Increasing Cost of Non-Compliance

The inevitability of the age of regulation has been made concrete by major global and local financial collapses. The Thodex scandal in Turkey is one of the most important examples of how the lack of transparency in centralized exchanges can increase systemic risks. Thodex's control of user assets off-chain prevented investors from independently verifying the security of their assets. Similarly, FTX's misuse of customer assets led to billions of dollars in losses. These crises have proven that independent Proof of Reserves (PoR) audit systems and mandatory transparency mechanisms are critical financial security tools that can detect fraud early on.

The classification of KVHSs as financial institutions has fundamentally changed the logic behind calculating Administrative Monetary Penalties (AMPs) to be imposed in case of violations. According to MASAK regulations, in the event of a breach of Know Your Customer (KYC) and Suspicious Transaction Reporting (STR) obligations, the penalty is applied at twice the basic APC amount, with a minimum of five percent of the transaction amount subject to the breach.

1.2.1. Impact of Legal Status Change on Corporate Governance

For KVHSs, this cost structure transforms compliance investments from a mandatory cost element into a strategic protection mechanism that ensures corporate continuity. As of 2024, the basic penalty upper limits exceeding 209,985,748*TL* pose a potential bankruptcy risk for KVHSs in the event of compliance deficiencies intersecting with high transaction volumes.

Graduated sanctions are applied to KVHSs that violate their obligations to establish a Compliance Program: first a written warning, then an administrative penalty (IPC), and if the deficiency is not remedied, the penalty is doubled. If the deficiency is not remedied after the second administrative penalty, the situation is reported to the relevant authority (SPK) for the revocation of the operating license. This chain of responsibility demonstrates that compliance is not merely an operational cost item but also a central corporate governance function under the responsibility of the Board of Directors.

1.3. The Strategic Value of Compliance and Vinu Digital's Positioning

Regulatory compliance has become a strategic competitive advantage for KVHSs, demonstrating market reliability and corporate maturity. In this new paradigm, KVHSs must simultaneously meet MASAK's legal requirements, SPK's operational standards, and TÜBİTAK's advanced technical criteria.

Integrated solutions such as Vinu Digital combine these complex obligations with an end-to-end manageable and auditable technical architecture. This approach ensures that KVHSs not only meet legal requirements but also provide the highest level of operational sustainability and financial security.

II. KVHS BASIC OBLIGATIONS AND GOVERNANCE FRAMEWORK

2.1. Establishment and Custody Principles Under the Capital Markets Board

The Capital Markets Board plays a central role in regulating the crypto asset market in Turkey. Crypto asset service providers must be established as joint-stock companies in accordance with the Board's circulars and meet high minimum capital adequacy requirements.

The SPK's area of responsibility covers ensuring compliance with the services offered by exchanges and operational standards. Institutions providing Crypto Asset Custody Services are also included in the definition of KVHS. Platforms are required to store all of their customers' crypto assets through a custody institution. Custody institutions must take the necessary measures to identify platform customers, but there is no requirement for the customer to sign a separate agreement with the custody institution.

2.2. Six Core Components of the MASAK Compliance Program and Corporate Responsibility

Law No. 5549 requires CRFIs to implement an effective compliance program based on a risk-based approach. According to the Compliance Regulation, the program has six core components, and the board of directors is ultimately responsible for the effective implementation of this program:

1. Development of Institutional Policies and Procedures.
2. Implementation of Risk Management Activities.
3. Implementation of Monitoring and Control Activities.
4. Implementation of Training Activities.
5. Implementation of Internal Audit Activities.
6. Establishment of a Compliance Unit and Appointment of a Compliance Officer and Compliance Officer Assistant.

The Compliance Officer (CO) should report to the board of directors and have the authority to request any information and documentation related to their area of responsibility from all departments of the organization (Legal, IT, Finance). This structure emphasizes that compliance is more than just an operational unit; it is a central control and assurance function of corporate governance.

2.3. Enhanced Customer Risk Management: PEP Management and Source of Funds Identification

CISs should establish a risk management policy based on customer risk, service risk, and country risk, taking into account the nature of their activities. When high-risk situations are identified, enhanced measures should be applied in proportion to the risk

2.3.1. Politically Exposed Person Management

Identification of Politically Exposed Persons (PEPs) is mandatory. PEPs are natural persons who hold high-level public office in their home country or in a foreign country, either through election or appointment. The enhanced measures applied to business relationships established with PEPs are as follows:

1. Entering into or continuing a business relationship **must be subject to the approval of a senior officer.**
2. Reasonable measures must be taken to determine the source of funds belonging to or processed by these individuals.
3. The business relationship must be kept under close scrutiny.

2.3.2. Legal Consequences of Risk Classification

MASAK requires that the customer's financial profile (business, occupation, income, estimated transaction volume) be obtained during identity verification. This comprehensive data collection creates the customer's initial risk profile and plays a

critical role in determining whether the transaction is consistent with the customer's financial profile in future Suspicious Transaction Report (STR) decisions.

Requiring high-risk transactions to be approved by a "senior official" shifts the legal responsibility for every risky decision up the corporate hierarchy. Vinu Digital's risk management system automates risk classification by integrating demographic risk scores and FATF/PEP indicators, providing managers with the vital data they need to make informed decisions before assuming legal responsibility.

➤ **III. TECHNOLOGICAL COMPLIANCE ARCHITECTURE: ADVANCED CUSTOMER IDENTIFICATION**

3.1. Remote Identity Verification Procedures: MASAK's Enhanced Measures

KVHSs can establish ongoing business relationships with their customers using remote identity verification methods. However, this process must be carried out within the framework of enhanced measures in accordance with the MASAK General Communiqué (No. 19). It is essential that the method be online, uninterrupted, visual, and real-time, and that the entire process be recorded for auditing purposes. It is accepted that KYC processes based on simple document uploads are unreliable and that an advanced infrastructure is therefore mandatory.

3.1.1. Mandatory Customer Profile Data

In remote identity verification, comprehensive customer profile data must be collected, including not only identity information but also the purpose and nature of the business relationship, estimated transaction volume, number of transactions, and average income information. This data is used to conduct an initial risk assessment of the customer and decide whether to enter into a business relationship.

3.2. Mandatory Technical Components: NFC, Biometric Liveness, and NVI Integration

Minimum technical controls are mandatory for the eKYC process for KVHSs:

- **NFC Reading and Verification:** The identity document must be verified using near field communication. This proves the physical integrity of the identity document by enabling chip-based verification.
- **MRZ/Hologram Verification:** If verification is not possible, at least four security features on the document must be verified in terms of shape and content.
- **Biometric Comparison and Liveness Detection:** A biometric comparison must be made between the person's face and the photo on their ID document, and additional measures (Liveness) must be taken against fake face technology.
- **NVI/KPS Verification:** Information such as the Turkish ID number, first name, last name, and date of birth must be verified through the Ministry of Interior's General Directorate of Population and Citizenship Affairs (NVI) Identity Sharing System (KPS) database.

Vinu Digital's eKYC module (Identity Verification) directly meets these mandatory

security standards with advanced technical details such as NFC reading, MRZ/Hologram verification, and Liveness detection.

3.3. Special Restrictions: Privacy-Based Assets and Initial Financial Transaction Requirement

MASAK has imposed special restrictions on remote identity verification:

- **Privacy-Based Asset Ban:** It is **strictly prohibited** for FCA entities facilitating the purchase, sale, or storage of privacy-based crypto assets to perform remote identity verification.
- **First Financial Transaction Requirement:** For establishing an ongoing business relationship, the first financial transaction, including deposits and withdrawals, must be made through a **bank or credit card account** that matches the customer's identity information. This requirement provides an additional layer of security by linking the digital identity to the traditional, regulated financial system.
- **Compensation for NFC Failure:** If the identity document cannot be verified using NFC, requiring the first financial transaction to be made through another financial institution that applies the principles of customer identification increases operational complexity in the absence of investment in advanced technical infrastructure such as NFC/MRZ.

IV. SUPERVISION AND CONTROL MECHANISMS FOR CRYPTO ASSET TRANSACTIONS

4.1. Travel Rule and Transfer Requirement

The international standard "Travel Rule" has been incorporated into Turkish legislation through Article 24/A of the MASAK Measures Regulation. This rule is mandatory for crypto asset transfers of fifteen thousand Turkish Lira (15,000TL) or more brokered by KVHSs. The rule requires that the necessary and accurate information about the sender be included in the transfer messages along with the necessary information about the recipient.

4.1.1. Mandatory Information and Technical Transmission

Transfer messages must contain, at a minimum, verified information about the sender and information about the recipient.

It is essential that information is sent simultaneously and securely with the transfer. Vinu Digital's Data Transfer Module uses international standards such as **JSON-LD** and **VMBSD** to transmit Travel Rule messages. Data confidentiality and integrity are ensured using **AES-256 encryption** and the **TLS 1.3** security protocol. The technical infrastructure's compliance with international standards minimizes the risk of the transfer being returned by the recipient KVHS due to missing mandatory information.

4.3. Transfer Restrictions to Unregistered Wallets

MASAK applies stricter measures to withdrawals made to wallets not registered with any KVHS in order to manage money laundering risks. These restrictions aim to prevent high-risk transfers by limiting the rapid movement of funds.

Transaction Type	Rule Application	Minimum Delay Time
First Crypto Withdrawal to an Unregistered Wallet	Enhanced Measures	At least 72 hours (to minimize fraud risk)
Subsequent Crypto Withdrawal to an Unregistered Wallet	Enhanced Measures	At least 48 hours (after a purchase, trade, or deposit transaction)

4.3.1. Stable Crypto Asset Limits

Daily limits of **\$3,000 USD** and monthly limits of **\$50,000 USD** are mandatory for stable crypto asset withdrawal transactions. For stable transfers between KVHSs where the Travel Rule applies, these limits may be doubled (Daily \$6,000 USD / Monthly \$100,000 USD). This flexibility encourages KVHSs to work with compliant platforms.

4.4. Transaction Description Requirement and Documentation of Asset Source

Cryptocurrency Service Providers (CSPs) must obtain from the customer a transaction description of at least **20 characters in length** for all cryptocurrency asset transfer transactions. Additionally, platforms are obligated to periodically collect documents from customers that demonstrate the source of the assets used in the transaction. These obligations are critical for proving the legal and economic purpose of the transaction in the event of a potential MASAK investigation.

➤ V. AUTONOMOUS RISK MONITORING AND SUSPICIOUS TRANSACTION REPORTING PROCESSES

5.1. Risk-Based Approach and Dynamic Customer Profile

CISs must continuously monitor whether transactions carried out by their customers are consistent with information about their profession, financial situation, and funding sources. Monitoring and control activities must continuously assess not only the transaction flow but also whether the customer is a Person of Public Influence and their connection to international lists.

5.2. Autonomous Monitoring Systems: Rule Engines and ML-Based Anomaly Detection

The requirement to fulfill the Suspicious Transaction Reporting obligation "immediately" highlights the inadequacy of processes dependent on manual oversight. Therefore, KVHSs must use advanced, autonomous technical infrastructure.

Vinu Digital's Transaction Monitoring System is designed to meet this need (refer to Vinu Digital visuals):

- **Rule Engine:** Detects violations of specific transaction limits or behavior patterns using threshold and pattern-based rules.
- **Machine Learning:** ML-based anomaly detection algorithms such as **Scikit-learn** and **TensorFlow** identify complex and previously unknown illegal transaction patterns in large data sets in real time.

This automation maximizes the speed of AML analysis, providing protection against potential administrative penalty risks exceeding 200 million TL.

5.3. Real-Time Risk Scoring and Integration with PEP/FATF Watch Lists

Risk classification should be automated and data-driven to support compliance decisions for KYC processes. Vinu Digital's Risk Management Module creates a dynamic customer risk score using demographic data and FATF/PEP Indicators. This automated scoring enables the flagging of customers or beneficial owners as PEPs, supporting the application of enhanced measures and the process of submitting high-risk transactions for senior management approval.

5.4. Management of SIB Obligations and Prohibition on Tipping-Off

It is essential that no one, including the parties involved in the transaction, disclose that a suspicious transaction report has been filed with MASAK. Those who violate this confidentiality obligation risk imprisonment for one to three years and a fine of up to five thousand days. This situation demonstrates that rapid and confidential automation, which minimizes human intervention in the FIU process, is not only an operational preference but also a legal requirement.

Category	Sub-Function	Description	Technical Detail
Identity Verification	Document Scanning	AI-powered document scanning and verification.	OCR engines, AI/ML algorithms for document analysis.
	API Scanning	Real-time scanning of API endpoints for suspicious activity.	API gateways, AI/ML algorithms for anomaly detection.
	Biometric Scanning	Facial recognition and biometric verification.	Facial recognition software, AI/ML algorithms for biometric analysis.
KYC/AML	Customer Onboarding	Automated customer onboarding process.	AI/ML algorithms for customer risk scoring, document verification.
	Transaction Monitoring	Real-time monitoring of transactions for suspicious activity.	AI/ML algorithms for transaction pattern analysis, rule engines.
	Sanctions Screening	Screening of customers and transactions against sanctions lists.	Sanctions lists, AI/ML algorithms for matching.
Data Transfer	Secure Transfer	Secure transfer of data between systems.	Encryption, secure protocols.
	API Transfer	Transfer of data via API endpoints.	API gateways, secure protocols.
	Cloud Transfer	Transfer of data to cloud storage.	Cloud storage, secure protocols.

Category	Sub-Function	Description	Technical Detail
Identity Verification	Document Scanning	AI-powered document scanning and verification.	OCR engines, AI/ML algorithms for document analysis.
	API Scanning	Real-time scanning of API endpoints for suspicious activity.	API gateways, AI/ML algorithms for anomaly detection.
	Biometric Scanning	Facial recognition and biometric verification.	Facial recognition software, AI/ML algorithms for biometric analysis.
KYC/AML	Customer Onboarding	Automated customer onboarding process.	AI/ML algorithms for customer risk scoring, document verification.
	Transaction Monitoring	Real-time monitoring of transactions for suspicious activity.	AI/ML algorithms for transaction pattern analysis, rule engines.
	Sanctions Screening	Screening of customers and transactions against sanctions lists.	Sanctions lists, AI/ML algorithms for matching.
Data Transfer	Secure Transfer	Secure transfer of data between systems.	Encryption, secure protocols.
	API Transfer	Transfer of data via API endpoints.	API gateways, secure protocols.
	Cloud Transfer	Transfer of data to cloud storage.	Cloud storage, secure protocols.

VI. TÜBİTAK CRITERIA: CRITICAL INFORMATION SYSTEMS SECURITY AND WALLET ARCHITECTURE

The information systems and technological infrastructure of KVHSs must comply with strict criteria published by TÜBİTAK, which is authorized by the Capital Markets Board. These criteria focus particularly on the protection of crypto asset private keys.

6.1. Cold and Hot Wallets: Mandatory Use of Secure Hardware Module (HSM)

The security of private keys is critical in crypto asset storage services.

- **Cold Wallet:** This wallet technology involves critical operations, such as signing crypto asset transfers, being performed in isolated environments using physical or technical **air gaps** that require intervention by authorized personnel.
- **Hot Wallet:** Even in these wallets that can be operated online, private keys or key fragments must be generated and processed in a secure environment or **Secure Hardware Modules**.

HSMs protect the entire lifecycle of keys, from generation to decommissioning. When physical tampering is detected, HSMs must securely erase the cryptographic keys and security data stored within them.

6.2. HSM Certification Standards: FIPS 140-3 and EN 419221-5

Cryptocurrency exchanges shall use HSMs in their cold wallets that have been tested according to at least **ISO/IEC 19790 Level-3** and possess a valid certificate.

Compliance with internationally recognized security standards is essential:

- **FIPS 140-3:** Published by the US National Institute of Standards and Technology, this standard, which contains security requirements for cryptographic modules, is important for KVHSs.
- **FPT_EMS:** It is recommended that HSMs include the FPT_EMS security requirement, which evaluates the adequacy of measures taken against side-channel attacks such as electromagnetic emissions and simple power analysis.

As a temporary provision, FIPS 140-2 certified modules procured from abroad may be used until December 31, 2026, provided that a commitment is obtained from the manufacturer.

6.3. Critical Software Security: EAL4 Common Criteria Evaluation

The security of critical software is as important as hardware security. Software that performs wallet access control and policy controls, as well as critical software such as Inter-Network Transition Systems, must be tested according to nationally or internationally recognized protection profiles and obtain a test report based on at least an **EAL4** level Common Criteria Evaluation. The EAL4 level proves that the product has been methodically designed, tested, and reviewed.

6.4. Cold Wallet Isolation: Air Gap and Inter-Network Transition

The isolation of private keys in cold wallets from internet-connected systems is a critical requirement. This isolation must be achieved using **Inter-Network Transition Systems** that provide data transmission control through physical air gaps or electronic methods.

If data transmission is automated using CDS, these tools must also be **evaluated at least at EAL4 level** by TÜBİTAK, and a test report must be obtained. These systems should only allow the two-way transfer of predefined data.

6.5. Critical Compliance Period: March 31, 2026 Technical Compliance Deadline

TÜBİTAK has set the deadline for KVHSs to comply with Cold Wallet Security Criteria, Access Control, and HSM Criteria as **March 31, 2026**. This date is a critical milestone for KVHSs to complete these comprehensive and capital-intensive infrastructure projects. TÜBİTAK's elaboration of these technical criteria demonstrates that the business of crypto asset custody is being addressed at the national critical infrastructure level.

➤ VII. CORPORATE GOVERNANCE, DATA MANAGEMENT, AND AUDITABILITY

7.1. International Security Certifications: ISO 27001 and SOC 2 Type II

In addition to legal requirements, compliance with international standards is important to increase market confidence and demonstrate operational robustness. Vinu Digital's infrastructure embraces certifications such as **ISO 27001** for Information Security Management and **SOC 2 Type II** for Service Organization Controls. This demonstrates that KVHSs meet the highest global standards for information security and auditability.

KVHSs must request assurance reports compliant with international standards such as ISO 27001 or SOC 2 Type II from external sources providing cloud computing or data center services.

7.2. Centralized Audit Log Management with Access and Authorization Control

Ensuring auditability is fundamental in corporate governance. Personnel authorization must be provided through **Role-Based Access Control** for platform security.

One of the most critical requirements is that all transactions, risk assessments, and notifications are recorded in an immutable **Audit Log**. This mechanism legally ensures compliance with the **8-year** data retention and presentation obligation mandated by Law No. 5549 of MASAK.

7.3. Legal Data Retention Obligation and Retention Period

MASAK requires that information and documents related to identity verification, transaction records, and all other obligations be securely retained for at least **8 years** from the transaction date. In particular, all audit trail records for transactions conducted via Inter-Network Transition Systems used for Cold Wallet isolation must be stored for at least **5 years** in a manner that ensures integrity control and redundancy.

7.4. Penetration Tests and Cyber Security Insurance

KVHSs must conduct regular scanning activities at intervals determined based on risk assessment and threat simulation studies at least once a year to identify

security vulnerabilities in information systems. To manage financial risks, it is recommended that KVHSs obtain cybersecurity insurance that covers potential financial losses arising from possible cyberattacks, data breaches, and business continuity interruptions stemming from information security risks.

VIII. CONCLUSION AND STRATEGIC ROADMAP FOR KVHS LEADERS

The era of regulation for crypto asset service providers signifies a necessary transformation from an operational and technological perspective. MASAK's KYC/AML and ŞİB obligations, SPK's establishment and custody standards, and TÜBİTAK's critical infrastructure security criteria are fundamentally changing the business model of KVHS and turning compliance into a strategic building block that can be converted into a competitive advantage.

8.1. TÜBİTAK Critical Information Systems Compliance Schedule and Standards

The most critical technical schedule and standards that KVHSs need to focus their capital and human resource investments on in the short term are as follows:

TÜBİTAK Critical Information Systems Compliance Schedule and Standards

Technical Requirement Area	Mandatory Standard / Criteria	Compliance Period / Deadline	Critical Role:
Cold Wallet & HSM	ISO/IEC 19790 Level-3 / FIPS 140-3, Tamper Response	31.03.2026	Key Custody Security
Critical Software Security	EAL4 Common Criteria Evaluation	Completion Required	Wallet Access and Policy Control
Cold Wallet Isolation	Air-Gapped / EAL4 Certified CDS	31.03.2026	Isolation from Internet Connection
Record Retention	Audit Log, Integrity and Redundancy	At least 8 years (MASAK) / 5 years (CDS)	Auditability and Legal Submission

8.2. Critical Action Plan for KVHS Leaders

- 1. Urgent Strengthening of Technical Infrastructure:** HSM procurement and integration must be completed by March 31, 2026, and EAL4-certified Inter-Network Transition Systems or physical air gap isolation must be provided for cold wallets.
- 2. Tightened Identity Verification and Restrictions:** NFC reading, biometric liveness, and NVİ integration must be mandatory in remote identity verification processes. Remote identity verification activities that facilitate privacy-based crypto assets must be stopped immediately.

3. Travel Rule and Transfer Flow Optimization: JSON-LD/VMBSD-compliant secure messaging infrastructures must be established for transfers exceeding the 15,000TL threshold. **48/72-hour transfer delays** for unregistered wallets should be integrated into the operational flow, and stable asset limits should be strictly enforced.

4. Autonomous AML and Risk Monitoring Investment: ML-based anomaly detection and rule engines should be integrated to ensure "immediate" compliance with AML obligations. Continuous scanning against PEP/FATF lists should support senior management approval processes.

5. Corporate Assurance and Audit: Audit Log systems that cannot be altered must be established to comply with MASAK's 8-year retention obligation. Corporate reliability must be certified with certifications such as ISO 27001 and SOC 2 Type II.

Integrated platforms such as Vinu Digital enable CSDs to manage this complex and dual compliance pressure, transforming legal requirements into operational excellence. In the new era, CSDs that demonstrate reliability and technological competence in the crypto asset market will overcome the challenges posed by regulations and establish themselves as industry leaders.

**Address**

Yaşamkent Mahalesi, 3250. Cad. 6C0
Çankaya/Ankara
Mersis No: 0925125517000001

E-Mail

info@vinu.com.tr

Phone

0 850 640 15 50

Web Site

vinu.com.tr