AML Controls for Crypto & High-Risk Clients

WWW.HPTGROUP.COM
12 RUE LE CORBUSIER, 1208 GENEVA, SWITZERLAND

Executive Summary

Engaging with crypto-related entities, high-risk clients, and cross-border digital assets requires enhanced AML safeguards. Traditional due diligence methods are often insufficient due to the pseudo-anonymous, high-velocity, and borderless nature of crypto transactions.
This guide outlines mandatory and recommended risk mitigation procedures for onboarding and managing high-risk clients, especially those operating in or exposed to the digital asset sector.

1. Client Risk Identification – Who Qualifies as High-Risk?

Entities and individuals are classified as high-risk if they meet any of the following criteria:

- Involved in Virtual Asset Services (VASPs) such as exchanges, custodians, or OTC desks
- Operate in or are incorporated in high-risk jurisdictions (FATF grey/blacklist)
- Politically Exposed Persons (PEPs) or those with known exposure to corruption risk
- Use complex legal structures, shell entities, or offshore layering
- Unverifiable source of wealth or source of funds
- Subject of adverse media, regulatory sanctions, or investigations

2. Onboarding Controls for Crypto & High-Risk Clients

Control Category	Required Measures
KYC & Identity Verification	Multi-level ID verification, facial biometrics, liveness checks, utility bills
Beneficial Ownership	Full disclosure and verification of UBOs (25%+)
Source of Funds / Wealth	Mandatory documentation, blockchain transaction tracing, wallet screening
PEP & Sanctions Screening	Daily automated screening against global watchlists
Business Model Validation	Obtain and assess whitepapers, operational websites, licenses, or blockchain use
Jurisdictional Review	Classify based on FATF risk lists and local regulatory alignment
Crypto Wallet Screening	Use of tools like Chainalysis, Elliptic, or CipherTrace to screen wallet addresses
IP Address & Geo-Fencing	Log and block access from sanctioned or embargoed countries

3. Ongoing Monitoring & Behavioral Triggers

High-risk clients must be subject to intensified ongoing monitoring, including:

- Transaction pattern analysis: Volume, frequency, counterparties
- Wallet activity tracking: Cross-referencing blockchain activity with client profile
- Crypto-to-fiat conversion reviews: Use of exchanges, mixers, privacy coins
- Jurisdictional routing: Funds or traffic routed through high-risk or secrecy jurisdictions
- Deviation from known behavior: Sudden increases in transaction volume, counterparties, or asset types

4. Enhanced Due Diligence (EDD) Documentation

EDD files for high-risk or crypto clients should contain:

- Source of Wealth Declaration (narrative + evidence)
- Source of Funds Trail (bank statements, blockchain explorer printouts)
- Business Model Analysis for VASPs or token projects
- Technology Stack Review (for DeFi or protocol entities)
- Ultimate Beneficial Owner (UBO) map, including legal entity chart
- Public wallet addresses + origin validation

5. Red Flags Specific to Crypto Activities

Red Flag	Risk Implication
Use of privacy coins (e.g., Monero, Zcash)	Obfuscation of transactional transparency
Mixing or tumbling services	Attempt to launder funds through anonymity
Transactions to/from sanctioned jurisdictions	Possible sanctions evasion
Use of unlicensed/unregistered exchanges	Counterparty risk and lack of regulatory recourse
Structuring below thresholds	Avoidance of monitoring and reporting
Newly created wallets with large deposits	Possible money mule or laundering operation

6. Governance & Escalation Procedures

- MLRO Approval is required before onboarding any high-risk or crypto-related client
- All red flags must be escalated to Compliance for review and potential SAR filing
- Automated monitoring systems must be calibrated specifically for crypto anomalies
- Maintain an audit trail of all crypto address screenings, onboarding decisions, and compliance notes

7. Training & System Readiness

- Staff must undergo crypto-specific AML training covering typologies, chain analysis, and risk indicators
- Systems must support wallet screening, smart contract interaction tracking, and cross-chain behavior mapping
- Continuous review of regulatory guidance from FATF, FinCEN, FCA, and ESMA is mandatory

8. Key Tools for Compliance Teams

Tool / Function	Examples
Blockchain Forensics	Chainalysis, Elliptic, TRM Labs, CipherTrace
Sanctions & PEP Screening	World-Check, Dow Jones Risk, ComplyAdvantage
KYB / Legal Entity Verification	Dun & Bradstreet, KYB360, LexisNexis Entity Insights
Ongoing Monitoring	Transaction anomaly detection tools, case management software

Conclusion

Crypto and high-risk clients present unique compliance challenges that demand advanced tools, targeted training, and layered due diligence. A robust, risk-based AML framework not only reduces exposure but also protects operational licenses and institutional reputation.