Guide to Conducting AML Risk Assessment

Introduction

Conducting a risk assessment is a critical component of operating a cryptocurrency business. It helps identify, evaluate, and mitigate potential risks associated with money laundering, fraud, regulatory non-compliance, and other financial crimes. This guide provides a step-by-step approach to conducting a comprehensive risk assessment tailored for crypto businesses.

As the money laundering reporting officer (MLRO), it's imperative to keep up to date by reading relevant materials such as those listed to help assess the risks associated with your firm. The MLRO must carry out a firm-wide risk assessment on a periodic basis.

Step 1: Understand Regulatory Requirements

Before starting the risk assessment, familiarise yourself with the relevant legal and regulatory frameworks, including:

- **Money Laundering, Terrorist Financing and Transfer of Funds Regulations (MLR 2017 & Amendments)**
- **Financial Action Task Force (FATF) Recommendations**
- **HM Treasury's National Risk Assessment**
- **Financial Conduct Authority (FCA) Guidelines**
- **Local and International Cryptocurrency Regulations**

Step 2: Identify Key Risk Areas

A risk assessment should focus on the primary risk areas for cryptocurrency businesses:

1. **Client Risk**
    - High-risk clients (e.g., PEPs, anonymous users, darknet market participants)
    - Use of privacy-enhancing technologies (e.g., mixers, privacy coins)
    - Clients with high transaction volumes and unclear sources of funds
2. **Geographic Risk**
    - Clients from high-risk jurisdictions (as per FATF and regulatory lists)
    - Transactions involving sanctioned countries
3. **Product & Service Risk**
    - Decentralized finance (DeFi) services
    - Initial Coin Offerings (ICOs) and token sales
    - Custodial and non-custodial crypto services
4. **Transaction Risk**

- High-value, rapid, or structured transactions
- Use of multiple wallets for layering activities

5. **Delivery Channels Risk**
    - Online-only interactions without in-person verification
    - Use of VPNs and anonymous access methods
6. **Proliferation Financing Risk**
    - Transactions potentially linked to weapons proliferation
    - Unexplained cross-border fund transfers

Step 3: Assess Risk Levels

For each risk area, categorize risks as **low, medium, or high** based on their potential impact and likelihood of occurring. This can be done using a risk matrix:

Risk Factor	Likelihood	Impact	Overall Risk Level
High-risk clients	High	High	High
Transactions from sanctioned jurisdictions	Medium	High	High
Use of privacy coins	High	Medium	High
Large, unexplained transactions	Medium	Medium	Medium
Remote-only customer onboarding	Low	Medium	Low

Step 4: Implement Mitigation Measures

Once risks are identified and categorized, apply appropriate mitigation strategies:

Risk	Mitigation Measures
High-risk clients	Enhanced Due Diligence (EDD), transaction monitoring
Transactions from high-risk countries	Geo-blocking, additional verification
Use of privacy coins	Restrict usage, require additional disclosures
Large transactions	Source of funds verification, flagging for review
Remote-only onboarding	AI-powered identity verification, live video calls

---

Step 5: Monitor and Review

Risk assessments should be an ongoing process, not a one-time activity. Implement a structured approach for monitoring and periodic reviews:

- **Real-time transaction monitoring** using blockchain analytics tools.
- **Periodic risk reassessments** to update policies based on evolving threats.
- **Staff training and awareness** to ensure employees understand emerging risks and compliance obligations.
- **Audit and reporting** to regulatory authorities as needed.

Step 6: Document and Report

Maintain detailed records of your risk assessment, including:

- The methodology used
- Identified risks and corresponding mitigation actions
- Results of ongoing monitoring and reviews
- Changes implemented in response to emerging threats

Ensure that the risk assessment is shared with key stakeholders, including compliance officers, senior management, and regulatory authorities where required.

Conclusion

A well-conducted risk assessment is vital for the success and compliance of a cryptocurrency business. By following these steps, businesses can proactively identify and mitigate risks, ensuring a secure and compliant operational environment.

Next Steps:

- Update risk assessments regularly to align with regulatory changes.
- Implement robust compliance programs to manage identified risks.
- Stay informed about emerging threats and evolving regulations in the crypto industry.