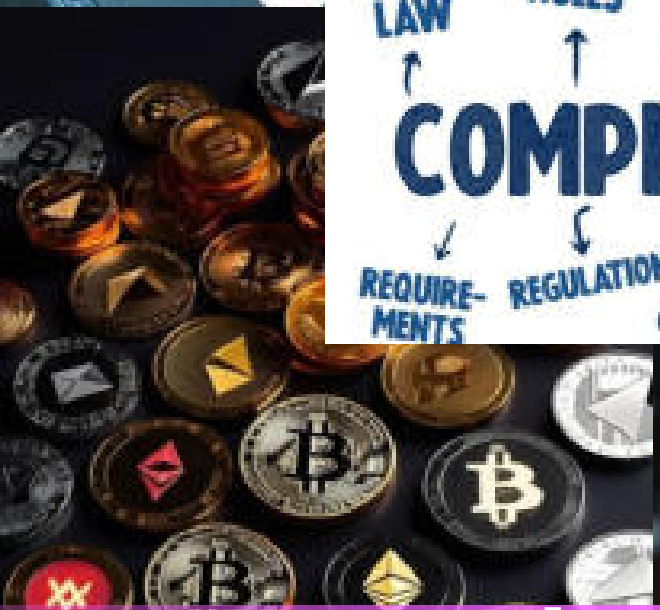
CRYPTO EXCHANGE/VASP COMPLIANCE AUDIT MANUAL



NOMINEE
ACAMS TODAY
ARTICLE of the Year
2025

Prepared By:-
Md Romel Sharif, CAMS, CCI

Overview and Intent

This Compliance Audit Manual is a fully comprehensive guide designed specifically for **Money Service Businesses [operating as Virtual Asset Service Providers (VASPs), including Crypto Exchanges, Digital Asset Exchange, Crypto Trading Platforms** which are treated as MSBs under U.S. law, requiring strict compliance audits] and auditors within the financial sector. It serves as both a practical toolkit and a regulatory compass for conducting effective, standardized, and risk-based compliance audits aligned with the highest expectations of financial integrity, customer protection, and legal conformity.

The intent of this manual is to support auditors in verifying whether MSBs maintain a robust compliance posture in alignment with applicable federal laws, risk-management principles, and global anti-financial crime standards. Through a methodical, checklist-driven approach, this guide enables auditors to objectively assess the presence, effectiveness, and execution of critical compliance controls across all core operational areas.

This manual has been carefully structured in accordance with a wide range of foundational U.S. federal laws and regulatory acts, including but not limited to:

1. **Anti-Money Laundering Act (AMLA), 2020**
2. **Corporate Transparency Act (CTA), 2021**
3. **FinCEN Travel Rule (31 CFR 103.33(g))**
4. **OFAC Sanctions Programs (SDN List, U.S. Treasury Department)**
5. **FATF 40 Recommendations (AML/CFT standards for VASPs)**
6. **State Money Transmitter Laws (MTL – varies by state)**
7. **New York Department of Financial Services (NYDFS) – BitLicense**
8. **Wolfsberg Group Principles on AML/CTF**
9. **Consumer Financial Protection Bureau (CFPB) Regulations**
10. **Unfair, Deceptive, or Abusive Acts or Practices (UDAAPs)**
11. **Gramm-Leach-Bliley Act (GLBA) – Privacy Rule & Safeguards Rule**
12. **California Consumer Privacy Act (CCPA), 2018**
13. **General Data Protection Regulation (GDPR – EU, if applicable)**
14. **Federal Trade Commission (FTC) Safeguards Rule**
15. **NIST Cybersecurity Framework**
16. **Truth in Lending Act (TILA)**
17. **Home Mortgage Disclosure Act (HMDA)**
18. **Homeowners Protection Act (HPA or PMI Cancellation Act)**
19. **Equal Credit Opportunity Act (ECOA)**
20. **Fair Credit Reporting Act (FCRA)**

21. **Fair Debt Collection Practices Act (FDCPA)**
22. **Real Estate Settlement Procedures Act (RESPA)**
23. **Secure and Fair Enforcement for Mortgage Licensing (SAFE) Act**
24. **Truth in Savings Act (TISA)**
25. **Consumer Leasing Act (CLA)**

In addition, the manual is aligned with the regulatory expectations and compliance frameworks established under:

Other relevant federal and state-level mandates applicable to MSBs

Scope and Applicability

This guide is intended for use by internal auditors, compliance officers, independent consultants, regulatory examiners, and authorized oversight personnel. It applies to all MSB functions engaged in automobile financing activities, such as installment loans, lease-to-own models, and related consumer financial services involving the transfer of funds, customer onboarding, credit risk assessment, and payment processing.

Audit Methodology

The audit framework within this manual follows a structured methodology consisting of:
Thematic Sectional Reviews
Risk-Based Scoring Models (Scoring matrix withheld for confidentiality)
Documentation Verification Checklists
Compliance Gap Indicators and Risk Flagging Protocols
Evidence-Based Sampling Recommendations
The audit sections are aligned with essential compliance domains including Governance, KYC/CDD/EDD, AML/CFT, Transaction Monitoring, STR/CTR Filing, Sanctions Screening, Employee Training, Technology Controls, Customer Risk Classification, Fraud Detection, and Ethical Culture Oversight.
Each section includes:
Defined Objectives
Comprehensive Checklist Tables
Mandatory Supporting Documentation
Detailed Auditor's Notes and Red Flags

Overview and Intent

Practical scenarios and audit triggers

Legal Disclaimer

While this guide provides a detailed compliance audit methodology, users are advised that it does not constitute legal advice. Institutions should ensure the final audit findings are cross-referenced with the latest regulatory developments and internal policies.

Final Note to Auditors

The effectiveness of an MSB's compliance program is not measured merely by the existence of policies, but by how well those policies are understood, implemented, and enforced. As such, your role as an auditor is not just to assess compliance on paper, but to evaluate compliance in practice. Use this manual not just as a checklist, but as a lens to assess whether the MSB's culture, systems, and staff behaviors reflect a genuine commitment to financial integrity, customer fairness, and regulatory accountability.

Let this guide empower you to uphold the principles of ethical finance and regulatory excellence in every audit engagement you conduct.

Document Submission Instructions

Submission Instructions for Compliance Audit

To proceed with the compliance audit efficiently, please review the instructions below and submit the requested documents accordingly:

1. Submission Deadline

Please submit all applicable documents within the stipulated time as discussed previously.
If you require additional time, kindly inform the audit team in writing before the deadline.

2. Submission Method

Documents can be submitted via any of the following secure channels:
Email (encrypted, if possible): xxx@fintracester.com
Secure Upload Portal (if provided)
Physical Handover in sealed envelope (by prior arrangement only)

3. Document Format

Preferred formats: PDF, Word, Excel, JPG/PNG
Ensure all files are clearly legible and complete
Large files may be compressed into a ZIP folder for convenience

4. File Naming Convention

To ensure clarity and efficient tracking, name your files using the reference codes from the audit checklist. Examples include:
D1_AMLCO_Appointment_Letter.pdf
D5_Customer_Risk_Matrix.xlsx
D9_KYC_SampleFiles.zip
If unsure about naming, use a descriptive title that matches the document's content.

5. Partial Availability

If your MSB does not possess a particular document listed in the checklist:
Do not delay submission of available documents
Clearly state in your email or cover note which items are not applicable or currently unavailable

Document Submission Instructions

Absence of specific items will be addressed as part of the audit observation and recommendation phase — it will not negatively impact the initial document collection process

6. Special Note for Small MSBs

For small-scale MSBs, the audit may be conducted via LIVE video conferencing, at the discretion and professional judgment of the assigned auditor.
In such cases:
A PDF copy of the draft audit report will be shared digitally
Upon receipt of all required documents, each sealed with the phrase "Original in Custody (OIC)" and signed by an authorized official,
The final signed original audit report will be securely dispatched to the auditee.

7. Point of Contact

For any queries, clarification, or submission confirmation, please contact:
Audit Coordinator: Md Romel Sharif
Email: xxx@fintracester.com
Phone/WhatsApp: +8801752179689
Organization: Fintracester Incorporated

Disclaimer & Confidentiality Note

This document has been prepared solely for the purpose of facilitating the collection of documentation necessary to conduct Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) compliance audit of the recipient Money Services Business (MSB). It is provided by the audit team (hereinafter referred to as "the Auditor") to assist the MSB in preparing and submitting documents relevant to its operations, risk profile, and internal controls.

The content, structure, and references within this document are strictly confidential and intended for use **only by the designated representatives of the MSB** to whom it is addressed. Unauthorized reproduction, distribution, forwarding, or disclosure to any external party, regulator, or service provider is **strictly prohibited** without prior written consent from the Auditor.

This document does **not** contain the internal audit methodology, scoring criteria, or proprietary risk assessment procedures of the Auditor. It does **not constitute legal, regulatory, or operational advice**, and should not be construed as such. The responsibility for ensuring regulatory compliance ultimately rests with the MSB and its management team.

The provision of this document does not create a legally binding agreement or guarantee the MSB's regulatory standing or audit outcome. The Auditor reserves the right to independently verify any information submitted, and to request additional documentation as deemed necessary.

All documentation submitted by the MSB in response to this request will be treated with the highest level of professional confidentiality and will be used **solely for the purposes of the current audit engagement**. Access to submitted materials will be limited to authorized audit personnel and will not be disclosed to any third party except as required by law or regulatory obligation.

By proceeding with the submission of documents, the MSB acknowledges and agrees to the terms outlined in this disclaimer.

Glossary for MSBs

SL NO		
		Government
1.	AFMLS	Asset Forfeiture and Money Laundering Section, Department of Justice
2.	BJA	Bureau of Justice Assistance, Department of Justice
3.	CFTC	Commodity Futures Trading Commission
4.	DEA	Drug Enforcement Administration, Department of Justice
5.	EOUSA	Executive Office of United States Attorneys, Department of Justice
6.	FBI	Federal Bureau of Investigation, Department of Justice
7.	FDIC	Federal Deposit Insurance Corporation
8.	Fed	Federal Reserve Board
9.	FinCEN	Financial Crimes Enforcement Network, Department of the Treasury
10.	HIDTA	High Intensity Drug Trafficking Area
11.	HIFCA	High Intensity Money Laundering and Related Financial Crime Area
12.	ICE	U.S. Immigration and Customs Enforcement
13.	INL	Bureau for International Narcotics and Law Enforcement Affairs, Department of State
14.	IRS-Cl	Internal Revenue Service -- Criminal Investigations, Department of the Treasury
15.	MLCC	Money Laundering Coordination Center, U.S. Immigration and Customers Enforcement, Department of Homeland Security
16.	NCUA	National Credit Union Administration
17.	OCC	Office of the Comptroller of the Currency, Department of the Treasury
18.	OCDETF	Organized Crime Drug Enforcement Task Force
19.	OFAC	Office of Foreign Assets Control, Department of the Treasury
20.	OJP	Office of Justice Programs, Department of Justice
21.	ONDCP	Office of National Drug Control Policy
22.	OTS	Office of Thrift Supervision, Department of the Treasury
		Securities and Exchange Commission
23.	SOD	Special Operations Division, Department of Justice
24.	USPIS	United States Postal Inspection Service
		U.S. Statutes, Laws and Reports
25.	BSA	Bank Secrecy Act
26.	IEEPA	International Emergency Economic Powers Act
27.	INCSR	International Narcotics Control Strategy Report

28.	MLCA	Money Laundering Control Act of 1986
29.	MLSA	Money Laundering Suppression Act of 1994

International Organizations and Related Terms

30.	APEC	Asia Pacific Economic Cooperation
31.	APG	Asia Pacific Group on Money Laundering
32.	CHFI	Committee on Hemispheric Financial Issues
33.	FATF	Financial Action Task Force on Money Laundering
34.	FIU	financial intelligence unit
35.	FSF	Financial Stability Forum
36.	GCC	Gulf Cooperation Council
37.	ILEA	International Law Enforcement Academy
38.	IFI	international financial institution
39.	IMF	International Monetary Fund
40.	NCCTs	non-cooperative countries or territories
41.	OAS	Organization of American States
42.	OECD	Organization for Economic Cooperation and Development
43.	OFC	offshore financial center

General Terminology

44.	BMPE	Black Market Peso Exchange
45.	GTO	Geographic Targeting Order
46.	MOU	Memorandum of understanding
47.	MSB	money services business

BSA Forms

48.	CMIR	Report of International Transportation of Currency or Monetary Instruments
49.	CTR	Currency Transaction Report
50.	FBAR	Foreign Bank Account Report
51.	SAR	Suspicious Activity Report
52.	SARC	Suspicious Activity Report for Casinos
53.	SAR-SF	Suspicious Activity Report for Securities Brokers and Dealers

TABLE OF CONTENTS

		Page No.
i	**Overview & Intent**	i
ii	**Submission Instruction**	iv
iii	**Disclaimer or Confidentiality Note**	vi
iv	**Glossary**	vii
v	**Table Of Contents**	ix

Section No.	Section Name	Purpose	Page No.
1	**Governance & Compliance Structure Audit**	To ensure the exchange has a strong governance framework with AMLCO, clear responsibilities, independence, and board oversight.	1
2	**AML/CFT Policy & Procedures Audit**	To verify AML/CFT policies are board-approved, updated, tailored to crypto risks, and aligned with FATF/FinCEN.	3
3	**Customer Due Diligence, KYC, and EDD Audit**	To confirm robust KYC/CDD procedures, Source of Funds checks, ongoing monitoring, and EDD for high-risk customers.	5
4	**Transaction Monitoring & STR/CTR Reporting**	To evaluate effectiveness of transaction monitoring, SAR/CTR filing, and reduction of false positives.	7
5	**Recordkeeping & Documentation Audit**	To ensure compliance records (KYC, transactions, SAR/CTR, logs) are retained and retrievable within timelines.	9
6	**Employee Training & Awareness Audit**	To confirm staff are trained on AML/CFT duties, crypto risks, reporting obligations, and effectiveness tested.	11
7	**Independent Testing & Internal Audit**	To assess whether AML/CFT controls are independently tested, findings documented, remediation tracked, and crypto risks reviewed.	13
8	**Sanctions & OFAC Screening**	To verify sanctions/PEP screening is automated, integrated, tested, and effective in blocking prohibited users/addresses.	15
9	**Product/Service Risk Assessment**	To ensure crypto products (spot, OTC, staking, NFTs, etc.) are risk-assessed, high-risk services get enhanced controls.	17

Section No.	Section Name	Purpose	Page No.
10	**Virtual Asset Wallet Risk Management**	To evaluate wallet risk management, including hosted vs. unhosted wallets, sanctions screening, verification, and withdrawal controls.	19
11	**Smart Contract & DeFi Protocol Risk Controls**	To confirm smart contracts/DeFi integrations are risk-assessed, audited, monitored for vulnerabilities, and restricted.	21
12	**Source of Funds & Proof-Origin Assessment**	To ensure high-risk customers' funds are verified, subject to stricter monitoring, escalation, and proof-of-origin checks.	23
13	**High-Risk Customer Handling**	To ensure high-risk customers (PEPs, privacy coin users, etc.) are identified, EDD applied, monitored, and escalated.	25
14	**Blockchain Analytics Tools Usage Audit**	To evaluate integration of blockchain analytics tools for detecting risky wallets, darknet links, and illicit activity.	27
15	**Crypto/Virtual Asset Transaction Monitoring**	To confirm automated monitoring of all crypto transactions with real-time alerts, tailored thresholds, and investigations.	29
16	**P2P and OTC Desk Risk Controls**	To assess AML controls in P2P/OTC operations, including KYC, SoF/SoW, fraud prevention, and dispute resolution.	31
17	**CIP Compliance — for fiat and crypto entry/exit**	To ensure Customer Identification Program (CIP) covers both fiat and crypto channels with enhanced checks.	33
18	**Whistleblower Policy**	To confirm employees have safe, anonymous, retaliation-free channels to report misconduct with escalation.	35
19	**Fraud Detection and Prevention Mechanism**	To ensure fraud detection tools exist to identify fake IDs, mule accounts, takeovers, with timely escalation.	37
20	**Cybersecurity & IT Security Controls**	To confirm strong IT/cybersecurity defenses safeguard customer data, wallets, and monitoring systems.	39
21	**Third-Party/Vendor Risk Management**	To ensure third-party vendors are risk-assessed, monitored, and contracts include AML/CFT obligations.	41

Section No.	Section Name	Purpose	Page No.
22	**Business Continuity & Disaster Recovery**	To verify continuity plans cover AML systems, data recovery, and crypto-related disaster scenarios.	**43**
23	**Regulatory Reporting & Correspondence**	To ensure timely, accurate responses to regulators, proper reporting logs, and documented communications.	**45**
24	**Data Privacy & Confidentiality Controls**	To verify customer data privacy, GDPR/CCPA compliance, and secure handling of sensitive information.	**47**
25	**Internal Controls & Segregation of Duties**	To confirm AML responsibilities are segregated, reducing conflicts of interest and ensuring accountability.	**49**
26	**Management Oversight & Board Reporting**	To ensure senior management and board review AML program performance, risks, and corrective measures.	**51**
27	**Risk-Based Approach (RBA) Framework**	To confirm the exchange applies risk-based methods for customer, product, and geographic risks.	**53**
28	**Cross-Border Transactions Risk**	To assess risks in cross-border crypto flows, high-risk jurisdictions, and additional monitoring requirements.	**55**
29	**Money Mule & Account Takeover Controls**	To verify detection/prevention of mule accounts, synthetic IDs, and compromised account activities.	**57**
30	**Correspondent & Institutional Relationships**	To ensure partner institutions are risk-assessed, monitored, and compliant with AML obligations.	**59**
31	**Law Enforcement & Regulator Cooperation**	To confirm proactive cooperation with authorities, timely data sharing, and support in investigations.	**61**
32	**Market Abuse & Manipulation Controls**	To ensure monitoring for pump-and-dump, insider trading, spoofing, and other abuse patterns.	**63**
33	**Crypto Travel Rule Compliance**	To verify Travel Rule implementation for crypto transfers, ensuring required sender/receiver data is shared.	**65**

Section No.	Section Name	Purpose	Page No.
34	**Crypto Custody & Cold Storage Controls**	To confirm strong custody practices, cold storage security, key management, and restricted access.	**67**
35	**Exchange Liquidity & Treasury Risk**	To assess liquidity, treasury controls, segregation of client funds, and risk of insolvency.	**69**
36	**Insider Trading & Staff Account Controls**	To verify controls on employee trading, account restrictions, and prevention of misuse of inside info.	**71**
37	**Cross-Platform & API Risk Controls**	To ensure API integrations and cross-platform operations are monitored for AML and fraud risks.	**73**
38	**Stablecoin & Token Listing Risk**	To confirm risk assessment of tokens/stablecoins before listing, including fraud and regulatory checks.	**75**
39	**NFT & Metaverse Risk Oversight**	To assess NFT/Metaverse-related AML risks, copyright misuse, and illicit activity controls.	**77**
40	**Crypto Derivatives & Leverage Risk**	To evaluate derivatives trading risks, leverage controls, and monitoring for abuse or manipulation.	**79**
41	**Exit Strategy & Offboarding Controls**	To ensure secure customer offboarding, withdrawal controls, and risk reviews at exit.	**81**
42	**Mergers, Acquisitions & Corporate Changes**	To confirm AML due diligence in M&A, restructuring, and leadership transitions.	**83**
43	**Overall AML/CFT Program Effectiveness Review**	To assess overall AML program effectiveness, gaps, and alignment with regulatory expectations.	**85**

Section 1: Governance & Compliance Structure Audit

Purpose: -To ensure the exchange has a strong governance framework with a designated AML Compliance Officer, clear responsibilities, independence from business, and oversight by the board/committee.

A. Audit Point Table

SL	Audit Point	Expected Compliance Practice	Risk Level	Auditor's Remarks
1.1	Is there a formally designated AML Compliance Officer (AMLCO/MLRO)?	Board-approved appointment; clearly named in policy and regulatory documents	Low / Med / High	
1.2	Does the AMLCO have adequate qualifications and experience?	CAMS, ACFCS, or similar certification; minimum 3–5 years AML experience	Low / Med / High	
1.3	Is the AMLCO functionally independent from business/commercial operations?	AMLCO should not be directly involved in sales, marketing, or finance	Low / Med / High	
1.4	Are the AMLCO's responsibilities clearly defined in a job description?	JD should include policy implementation, STR/CTR filing, training, reporting to board	Low / Med / High	
1.5	Does the AMLCO report directly to senior management or board?	Evidence of independent reporting line; ideally with quarterly updates to board	Low / Med / High	
1.6	Has the AMLCO received recent AML/CFT training (within last 12 months)?	Internal or external training (e.g., webinar, ACAMS conference, in-house session) documented	Low / Med / High	
1.7	Is there an up-to-date Organizational Chart showing reporting structure?	Clear visual diagram of who reports to whom, where AMLCO fits	Low / Med / High	
1.8	Is there a compliance committee or governance forum to oversee AML matters?	May include board audit committee, compliance forum, or senior risk committee	Low / Med / High	
1.9	Are there board meeting minutes reflecting AML/CFT oversight & discussion?	Board/Management meeting records showing AML review, SAR trends, regulatory updates, internal audits	Low / Med / High	
1.10	Are AML roles and responsibilities assigned across departments?	Responsibility matrix (e.g., who handles KYC, monitoring, STR filing, audit, training, etc.)	Low / Med / High	

B. Document Required: -

SL	Document Name	Description / What to Look For
D1	AMLCO Appointment Letter / HR Record	
D2	AMLCO Job Description (JD)	
D3	AMLCO Resume	Certifications
D4	Organizational Chart	
D5	AML Policy Document (AMLCO Responsibilities Section)	
D6	Board Meeting Minutes (AML topics highlighted)	
D7	Compliance Governance Structure Document	
D8	Compliance Training Attendance Sheet	
D9	AML Roles & Responsibilities Matrix	
D10	Reporting Calendar / Quarterly Update Log	

C. Notes for Auditor

- 1.1. If AMLCO is unnamed in policy or HR file, mark as High Risk
- 1.2. If there is no professional certification or insufficient experience, mark as Medium or High
- 1.3. If AMLCO is also responsible for revenue-generating operations, flag independence risk
- 1.5. If AMLCO reports to Finance/Operations instead of board or CEO, note as structural weakness
- 1.6. If there is no training record in last 12 months, I will raise risk and require immediate corrective action
- 1.7. Organizational chart must be dated and should clearly highlight AMLCO's reporting line
- 1.8. If no committee exists, or AML not on meeting agenda, consider oversight weak
- 1.9. Absence of AML topics in board minutes = likely governance gap
- 10. If roles are informal or undocumented, escalate risk and recommend a responsibility matrix

Section 2: AML/CFT Policy & Procedures Audit

Purpose: -To verify that AML/CFT policies are written, board-approved, updated annually, tailored to crypto risks, and aligned with FATF/Finchem requirements.

A. Audit Point Table

SL	Audit Point	Expected Compliance Practice	Risk Level	Auditor's Remark
2.1	Is there a written AML/CFT policy tailored to crypto operations?	Covers VASP-specific risks, DeFi/P2P exposure, wallet transfers, blockchain anonymity	Low / Med / High	
2.2	Is the AML policy board-approved and updated annually?	Latest version shows board sign-off and version history	Low / Med / High	
2.3	Are AML program elements clearly documented?	Must include AMLCO appointment, internal controls, training, and independent audit	Low / Med / High	
2.4	Are crypto-specific risks addressed in the policy?	Includes wallet-based risk, privacy coins, unposted wallets, chain hopping, tumblers	Low / Med / High	
2.5	Are procedures in place for STR/CTR filing under 31 CFR §1022?	Clear guidance on thresholds, timelines, escalation path	Low / Med / High	
2.6	Is there a procedure for Enhanced Due Diligence (EDD)?	Required for high-risk crypto users, foreign exchanges, PEPs	Low / Med / High	
2.7	Is onboarding, monitoring, and exit processes defined?	Includes thresholds for onboarding freeze, user deactivation, and escalations	Low / Med / High	
2.8	Are procedures aligned with FATF Recommendation 15 (Virtual Assets)?	Should explicitly state VA-specific obligations and blockchain monitoring duties	Low / Med / High	
2.9	Are crypto-transaction monitoring tools referenced in policy?	Policy names tools (e.g., Chain lysis, Elliptic, Score chain) and explains usage scope	Low / Med / High	
2.10	Is the policy accessible to all relevant employees?	Internal intranet, policy handbooks, compliance training portal	Low / Med / High	

B. Document Required: -

SL	Document Name	Description / What to Look For
D1	AML/CFT Policy Document (latest signed version)	
D2	Policy Revision History or Board Approval Memo	
D3	AML Program Overview Section (4 pillars	crypto context)
D4	Crypto Risk Addendum or VA-Specific Procedure Manual	
D5	STR/CTR Filing SOP	
D6	EDD Process Flow or Checklist	
D7	Monitoring & Exit Flowchart	
D8	FATF R.15 Compliance Mapping Sheet	
D9	Transaction Monitoring Tool Reference Page (in policy)	
D10	Policy Distribution Log or Internal Circulation Proof	

C. Notes for Auditor:

- If the policy lacks virtual assets and blockchain-specific threats, flag 2.4
- If STR/CTR procedure is generic or paper-based, mark 2.5 as weak
- If FATF R.15 is not explicitly mapped, raise a procedural compliance gap under 2.8
- If crypto tools (Chain lysis, TRM Labs, etc.) are in use but not mentioned in policy — note gap in 2.9
- Confirm 2.10 via staff interview or IT/internal distribution audit trail