COINPORT'S RISK ASSESSMENT AND MANAGEMENT MATRIX

Version 3.0 | Effective: 5 January 2026

Alignment with: Unified AML/CTF Program (Appendix 3 integrated)

RISK SCORING METHODOLOGY

- **Likelihood:** LOW (1) | MEDIUM (2) | HIGH (3)
- **Impact:** LOW (1) | MEDIUM (2) | HIGH (3)
- **Overall Risk Score:** Likelihood × Impact = Score (1-9)
- **Risk Rating:** LOW (1-3) | MEDIUM (4-6) | HIGH (7-9)

A. REGULATORY COMPLIANCE RISK

Item	Risk Description	Type	Likelihood	Impact	Risk Score	Control Measures	Program Reference
A.1	Failure to report suspicious matters (SMR)	Critical	Low	High	**HIGH**	• SMR procedures with 24hr (TF) / 3-day (ML) deadlines • Red Flag Indicator Sheet (Appendix 2) • AML/CTF CO escalation workflow	Section 22
A.2	Failure to monitor	Critical	Low	High	**HIGH**	• Automated transaction monitoring	Section 21

Item	Risk Description	Type	Likelihood	Impact	Risk Score	Control Measures	Program Reference
	customer transactions					• AMLBot blockchain analytics • Weekly Board review of transaction reports • Enhanced monitoring for high-risk customers	
A.3	Customer identification requirements not met	Major	Low	High	**HIGH**	• Electronic verification (KYC-AID, Sumsub) • Liveness detection • Risk-based CDD (Simplified/Standard/Enhanced)	Sections 31-42
A.4	Customer verification done improperly	Major	Low	High	**HIGH**	• Multi-source verification • Document authenticity checks • Discrepancy tolerance procedures (Section 46)	Sections 33-35
A.5	Third-party provider oversight failure	Major	Low	High	**HIGH**	• Quarterly third-party reviews • KYC-AID, Sumsub, AMLBot due diligence • Contractual AML/CTF obligations	Section 19
A.6	No AML/CTF Program in place	Major	Low	High	**HIGH**	• Board-approved unified Program (5 Jan 2026) • Annual independent review • Monthly Board reporting	Sections 2, 9
A.7	Failure to submit AML/CTF Compliance Report	Major	Low	High	**HIGH**	• Annual report due 31 March • AML/CTF CO responsible • AUSTRAC Online submission	Section 27
A.8	No AML/CTF Compliance Officer appointed	Major	Low	High	**HIGH**	• Nicanor Nuqui appointed as AML/CTF CO • Direct Board reporting • Independent authority	Section 10

Item	Risk Description	Type	Likelihood	Impact	Risk Score	Control Measures	Program Reference
A.9	Board oversight failure	Major	Low	High	**HIGH**	• Monthly Board meetings with AML/CTF CO • Quarterly risk reviews • Management accountability (2026 requirement)	Section 9
A.10	**Travel Rule non-compliance (NEW)**	Critical	Medium	High	**HIGH**	• Sumsub + Notabene implementation • VASP counterparty due diligence (Appendix 4) • NO threshold for VASP-to-VASP transfers • $10k threshold for self-hosted wallets	Section 25
A.11	**Sanctions screening failure (NEW)**	Critical	Low	High	**HIGH**	• Real-time AMLBot wallet screening • Daily customer re-screening • DFAT, UN, OFAC, EU, UK lists • PF sanctions included	Section 26
A.12	**Proliferation Financing (PF) risk unmanaged (NEW)**	Major	Low-Med	Medium	**MEDIUM**	• PF sanctions screening • Enhanced beneficial ownership for corporates • No business in PF-concern jurisdictions • Staff training on PF red flags	Sections 14A, 26.2

B. CUSTOMER TYPE RISK

Item #	Customer Type	Risk Score	Control Measures	Program Reference
B.1	**Individual – Standard Retail** (Australian,	**LOW (1)**	• Standard KYC (KYC-AID/Sumsub) • Annual review	Section 34

Item #	Customer Type	Risk Score	Control Measures	Program Reference
	employment income, <$10k/month)		• 55+ age fraud screening (Section 32.9) • Automated monitoring	
B.2	**Individual – Joint Account (same address, married)**	**LOW (1)**	• Verify both parties • Standard KYC procedures • Annual review	Section 34
B.3	**Individual – Joint Account (different surnames, same address)**	**MEDIUM (4)**	• Enhanced verification of relationship • Additional documentation • Certified copies if discrepancies	Section 34
B.4	**Individual – Joint Account (different addresses)**	**HIGH (7)**	• GENERALLY DECLINED • If approved: Senior management + Enhanced CDD	Section 34
B.5	**Sole Trader**	**LOW (1)**	• Business name verification • ABN check • Source of funds documentation	Section 34
B.6	**Company – Australian Domestic (standard)**	**MEDIUM (4)**	• ASIC database verification • Beneficial ownership (25% threshold) • Annual KYC review • Enhanced if complex structure	Section 35
B.7	**Company – ASX Listed / APRA-Regulated**	**LOW (2)**	• Simplified CDD procedure • Reduced beneficial ownership requirements • Annual reviews	Section 35(i)
B.8	**Company – Foreign Registered (ASIC)**	**MEDIUM (4)**	• ARBN verification • Country of incorporation risk assessment • Enhanced beneficial ownership	Section 35(iii)
B.9	**Company – Unregistered Foreign**	**MEDIUM-HIGH (6)**	• Foreign registration body verification	Section 35(iv)

Item #	Customer Type	Risk Score	Control Measures	Program Reference
			• Disclosure certificate may be required • AML/CTF CO approval	
B.10	Company - Corporate Directors	MEDIUM-HIGH (6)	• Multi-layer beneficial ownership • Ultimate individual ownership verification • Enhanced scrutiny for shell company indicators	Section 35, 43
B.11	Trust - Regulated (APRA, ASIC-registered MIS)	LOW-MEDIUM (3)	• Simplified verification • Regulatory database check • Trustee verification	Section 36(i)
B.12	Trust - Other (family, discretionary, unit)	MEDIUM (4)	• Trust deed verification • Settlor identification • Beneficiary identification (class or individual) • Trustee verification	Section 36(ii)
B.13	Trust - Custodian (AFSL holder)	LOW-MEDIUM (3)	• AFSL verification • Reporting Entities Roll confirmation • Underlying customer CDD attestation	Section 36(iii)
B.14	Self-Managed Super Fund (SMSF)	MEDIUM (4)	• ATO registration verification • Trustee identification • Pension phase verification	Section 36
B.15	Partnership	MEDIUM (4)	• Partnership agreement • All partner identification • Business activity verification	Section 38
B.16	Institutional Client (super fund, corporate treasury)	MEDIUM (4)	• Enhanced due diligence • Source of funds verification • Senior management approval	Section 30
B.17	Association / Registered Co-operative	LOW-MEDIUM (3)	• Incorporation verification • Committee member identification • Constitution review	Sections 39-40

Item #	Customer Type	Risk Score	Control Measures	Program Reference
B.18	**Government Body**	**LOW (2)**	• Legislative verification • Officer identification • Generally low risk	Section 41
B.19	**Agent (Power of Attorney)**	**MEDIUM (4)**	• Agent identity verification • Authorization documentation • Principal verification	Section 42
B.20	**Politically Exposed Person (PEP) - Australian/Int'l Org**	**MEDIUM-HIGH (6)**	• Board approval required • Enhanced CDD (source of wealth • Semi-annual review • Adverse media screening	Section 44
B.21	**Politically Exposed Person (PEP) - Foreign**	**HIGH (7-9)**	• Board approval mandatory • Enhanced CDD (source of wealth + funds) • Semi-annual review with AML/CTF CO sign-off • Weekly transaction monitoring	Section 44

C. DESIGNATED SERVICES & DELIVERY CHANNELS RISK

Item #	Risk Area	Risk Score	Control Measures	Program Reference
C.1	**Virtual Asset Exchange Services (Item 50A)**	**MEDIUM (4)**	• Buy/sell/exchange/custody of BTC, ETH, stablecoins • AMLBot blockchain analytics on all transactions • Sanctions screening (wallet-level) • Transaction limits based on customer risk	Section 15
C.2	**Non-Face-to-Face Onboarding (Digital Platform)**	**MEDIUM (4)**	• Electronic ID verification (KYC-AID, Sumsub) • Liveness detection • Device fingerprinting	Sections 32.6-32.9, 33

Item #	Risk Area	Risk Score	Control Measures	Program Reference
			• Multi-factor authentication • 55+ age fraud prevention calls	
C.3	**Instant Payment Integration (Monoova OSKO/PayID)**	**MEDIUM (4)**	• Real-time transaction monitoring • Duplicate payment detection • Bank account name matching • New customer 24-48hr hold • Graduated withdrawal limits	Sections 15.4, 21
C.4	**Blockchain-Based Transfers**	**MEDIUM (4)**	• AMLBot real-time screening • Sanctioned address blocking • Blacklisted exchange detection • Mixer/tumbler flagging • Darknet marketplace monitoring	Sections 15.4, 26.3
C.5	**Travel Rule - VASP-to-VASP Transfers (NO THRESHOLD)**	**MEDIUM-HIGH (5)**	• Sumsub + Notabene protocol • Counterparty VASP due diligence (Appendix 4) • Originator/beneficiary info collection • Non-responsive VASP escalation	Section 25
C.6	**Self-Hosted Wallet Transfers (≥$10,000 AUD)**	**MEDIUM-HIGH (6)**	• Enhanced due diligence mandatory • Wallet ownership demonstration • AMLBot risk assessment • AUSTRAC reporting • Senior management approval	Section 25.2 (Scenario 2)
C.7	**Cross-Border Remittances (Australia-Philippines)**	**LOW-MEDIUM (3)**	• Enhanced source of funds verification • Beneficiary identification (>$5k) • Travel Rule compliance • Structuring monitoring	Appendix 3 Section 4
C.8	**High-Value Transactions (>$50,000/month)**	**MEDIUM-HIGH (6)**	• Automatic Enhanced CDD trigger • Source of wealth documentation • Senior management approval • Semi-annual KYC refresh	Section 30
C.9	**Privacy Coin Conversions (Monero, Zcash)**	**HIGH (7)**	• **RESTRICTED OR PROHIBITED** • Enhanced monitoring if allowed • Immediate AML/CTF CO escalation	Appendix 2 (Red Flags)

D. GEOGRAPHIC & JURISDICTIONAL RISK

D.1 Customer Residence/Operations

Item #	Jurisdiction Category	Risk Score	Countries Included	Control Measures	Program Reference
D.1a	**Australia (Primary Operations)**	**LOW (1)**	Australia	• Full AUSTRAC compliance • Robust AML/CTF framework • Standard monitoring	Appendix 3 Section 4
D.1b	**FATF-Compliant (Low Risk)**	**LOW (1)**	UK, EU, USA, Canada, Singapore, Japan, NZ, most developed economies	• Standard CDD • Travel Rule compliance • Sanctions screening	Appendix 3 Section 4
D.1c	**FATF Grey List / Higher Risk**	**MEDIUM–HIGH (6)**	Philippines, Turkey, UAE, South Africa, Pakistan, Myanmar, others per current FATF list	• Enhanced due diligence • Additional source of funds verification • More frequent KYC reviews • AML/CTF CO approval	Appendix 3 Section 4
D.1d	**Sanctioned / Proliferation Concern Jurisdictions**	**HIGH (9) – PROHIBITED**	**North Korea, Iran, Syria, Cuba, Russia (certain sectors), Venezuela (certain sectors)**	• **NO BUSINESS ACCEPTED** • Immediate transaction block • Existing accounts suspended • SMR filing mandatory • AUSTRAC/DFAT notification	Sections 26, 14A
D.1e	**FATF Black List /**	**HIGH (9) –**	Per current FATF public statement	• **NO BUSINESS ACCEPTED** • Senior management	Appendix 3 Section 4

Item #	Jurisdiction Category	Risk Score	Countries Included	Control Measures	Program Reference
	Non-Cooperative	**PROHIBITED**	(Myanmar, etc.)	escalation if approached • Document and report	

D.2 Transaction Destination/Origin

Item #	Scenario	Risk Score	Control Measures
D.2a	**Domestic (Australia-to-Australia)**	**LOW (1)**	• Standard transaction monitoring • AMLBot blockchain screening
D.2b	**Australia to FATF-Compliant**	**LOW-MEDIUM (3)**	• Travel Rule compliance (if VASP) • Enhanced beneficiary verification • Purpose of transaction documentation
D.2c	**Australia to Grey List / Higher Risk**	**MEDIUM-HIGH (6)**	• Enhanced due diligence • Source of funds + purpose verification • Structuring monitoring • Consider SMR if suspicious
D.2d	**Any Sanctioned Jurisdiction**	**HIGH (9) – BLOCKED**	• **TRANSACTION REJECTED** • Sanctions violation protocols • Immediate DFAT/AUSTRAC notification

---

E. PROLIFERATION FINANCING (PF) SPECIFIC RISKS (NEW 2026)

Item #	Risk Description	Risk Score	Control Measures	Program Reference
E.1	**Corporate customer with links to PF-concern jurisdictions**	**MEDIUM-HIGH (6)**	• Enhanced beneficial ownership verification • Sanctions screening (UN, OFAC, DFAT PF lists) • No business with North Korea/Iran entities • Front company indicator screening	Sections 14A, 26.2

Item #	Risk Description	Risk Score	Control Measures	Program Reference
E.2	**Dual-use goods involvement**	**MEDIUM (4)**	• Customer business activity screening • Trade finance transactions (NOT offered by CoinPort) • Enhanced scrutiny if tech/chemicals/manufacturing	Section 14A.3
E.3	**Complex corporate structures (potential sanctions evasion)**	**MEDIUM (4)**	• Multi-layer beneficial ownership analysis • Shell company red flag screening • Ultimate individual ownership required • No clear commercial purpose = High Risk	Sections 14A, 43, Appendix 2
E.4	**State-owned enterprise connections (PF jurisdictions)**	**HIGH (9) – PROHIBITED**	• **NO BUSINESS WITH SOEs in North Korea, Iran** • Enhanced screening for indirect connections • SMR filing if identified	Section 14A.3

F. TECHNOLOGY & OPERATIONAL RISK

Item #	Risk Description	Risk Score	Control Measures	Program Reference
F.1	**Blockchain analytics tool failure**	**MEDIUM-HIGH (6)**	• AMLBot redundancy • Manual review backup procedures • Daily system health checks • Vendor SLA monitoring	Section 19 (Third Parties)
F.2	**Travel Rule system failure (from 31 March 2026)**	**HIGH (7)**	• Sumsub + Notabene dual implementation • VASP-to-VASP transaction hold if system down • Manual fallback procedures • Incident documentation	Section 25

Item #	Risk Description	Risk Score	Control Measures	Program Reference
F.3	**KYC verification system failure (KYC-AID, Sumsub)**	**MEDIUM (4)**	• Dual provider setup (KYC-AID + Sumsub) • Manual verification backup • New customer onboarding pause if systems down	Sections 19, 33
F.4	**Sanctions screening system failure**	**HIGH (8)**	• Real-time screening via AMLBot • Daily customer database re-screening • Manual sanctions list checks if system down • Transaction halt until resolved	Section 26
F.5	**Payment system compromise (Monoova)**	**MEDIUM (4)**	• Real-time fraud monitoring • Duplicate payment detection • Bank account name matching • Immediate escalation protocols	Section 15.4

G. EMPLOYEE & OPERATIONAL RISK

Item #	Risk Description	Risk Score	Control Measures	Program Reference
G.1	**Failure to screen employees**	**MEDIUM-HIGH (6)**	• AFP criminal history checks • Credit/bankruptcy checks • Reference checks (minimum 2) • Pre-employment verification	Section 17
G.2	**Inadequate staff training**	**MEDIUM (4)**	• Annual AML/CTF training mandatory • Induction training for new staff • Travel Rule training (2026) • PF red flags training • Training register maintained	Section 18
G.3	**Staff non-compliance with Program**	**MEDIUM (4)**	• Spot checks by AML/CTF CO • Disciplinary action framework • Culture of compliance (tone from	Section 17.5

Item #	Risk Description	Risk Score	Control Measures	Program Reference
			top) • Anonymous reporting channels	
G.4	**Insider threat (employee collusion)**	**LOW-MEDIUM (3)**	• Two-signature requirement for fund transfers • Segregation of duties • Transaction monitoring includes staff accounts • Regular access reviews	Section 17.1

H. BEHAVIORAL RED FLAGS & TRANSACTION PATTERNS

Item #	Red Flag Description	Risk Score	Action Required	Program Reference
H.1	**Customer reluctant to provide ID**	**MEDIUM-HIGH (6)**	• Enhanced CDD • Consider rejecting customer • SMR if suspicion formed	Appendix 2, Section 22
H.2	**Suspicious/altered documents**	**HIGH (7)**	• Document verification specialist review • Certified copies required • Consider rejecting • SMR likely required	Sections 34, 46
H.3	**Customer nervous/evasive during KYC**	**MEDIUM (4)**	• Additional verification questions • Enhanced monitoring • Document interaction • Consider 55+ fraud screening	Appendix 2
H.4	**55+ age with limited crypto knowledge**	**MEDIUM (4) - FRAUD VICTIM**	• **MANDATORY PHONE CALL (Section 32.9)** • Assess crypto understanding • Fraud warning if concerns • Account suspension if likely victim	Section 32.9

Item #	Red Flag Description	Risk Score	Action Required	Program Reference
H.5	Multiple account/wallet attempts	HIGH (7)	• Enhanced CDD • Investigate reason • Link analysis • Consider rejection	Appendix 2
H.6	Structuring under $10k threshold	HIGH (8)	• Aggregate related transactions • Enhanced monitoring • SMR filing • Consider TTR filing	Appendix 2, Section 23
H.7	Occupation inconsistent with transaction volume	MEDIUM-HIGH (6)	• Source of funds verification • Enhanced CDD • Ongoing monitoring	Appendix 2
H.8	Requests unusual secrecy	HIGH (7)	• Enhanced CDD • Senior management notification • Consider rejecting • SMR if suspicious	Appendix 2
H.9	Uses VPN to obscure location systematically	MEDIUM (4)	• Verify actual location • Cross-check with KYC address • Enhanced monitoring	Appendix 2
H.10	Multiple failed KYC attempts with different details	HIGH (8)	• Account suspension • Fraud investigation • SMR filing • Possible ban	Appendix 2
H.11	Rapid fund movement (deposit → immediate withdrawal)	HIGH (7)	• Transaction hold • Enhanced verification • Source of funds inquiry • SMR if suspicious	Appendix 2
H.12	Round number transactions ($5k, $10k, $50k exact)	MEDIUM (4)	• Pattern analysis • Aggregate with other red flags • Enhanced monitoring	Appendix 2
H.13	100%+ volume increase within 5 days	HIGH (7)	• Immediate enhanced CDD • Source of funds verification • Transaction review • SMR consideration	Section 30.6(b)(v)

Item #	Red Flag Description	Risk Score	Action Required	Program Reference
H.14	High-frequency trading inconsistent with profile	MEDIUM-HIGH (6)	• Verify trading experience • Source of funds • Enhanced monitoring	Appendix 2
H.15	Complex transaction chains (no economic rationale)	HIGH (8)	• Transaction purpose inquiry • Blockchain analytics deep dive • SMR filing	Appendix 2
H.16	Large cash deposits preference	HIGH (8)	• **CoinPort does NOT accept cash** • If discovered, immediate investigation • SMR filing	Appendix 2
H.17	Transactions with PEPs (customer not PEP themselves)	MEDIUM-HIGH (6)	• Enhanced monitoring • PEP relationship documentation • Purpose verification	Appendix 2

I. BLOCKCHAIN-SPECIFIC RED FLAGS (AMLBot Monitoring)

Item #	AMLBot Alert Type	Risk Score	Action Required	Program Reference
I.1	Deposits from mixers/tumblers (Tornado Cash, Wasabi, CoinJoin)	HIGH (9) – BLOCK	• **IMMEDIATE TRANSACTION BLOCK** • AML/CTF CO escalation • SMR filing mandatory • Customer account suspension	Appendix 2, Section 26.3
I.2	Wallet flagged as high-risk by AMLBot	MEDIUM-HIGH (6)	• Manual review by AML/CTF CO • Risk assessment documentation • Enhanced monitoring if approved • Rejection if severe	Appendix 2
I.3	Darknet marketplace connections	HIGH (9) – BLOCK	• **IMMEDIATE TRANSACTION BLOCK** • SMR filing mandatory • Account suspension • AUSTRAC notification	Appendix 2

Item #	AMLBot Alert Type	Risk Score	Action Required	Program Reference
I.4	**Sanctioned address interaction (OFAC SDN, DFAT, UN)**	**HIGH (9) – BLOCK**	• **IMMEDIATE TRANSACTION BLOCK** • Asset freeze • DFAT/AUSTRAC reporting • Legal counsel consultation	Sections 26.3, 26.4
I.5	**Blacklisted exchange interaction**	**MEDIUM-HIGH (6)**	• Manual review • Exchange reputation check • Enhanced monitoring or block • Document decision	Appendix 2
I.6	**Exchange hop patterns (rapid multi-exchange)**	**MEDIUM (4)**	• Pattern analysis • Purpose inquiry • Enhanced monitoring	Appendix 2
I.7	**Ransomware payment address**	**HIGH (9) – BLOCK**	• **IMMEDIATE TRANSACTION BLOCK** • SMR filing mandatory • Law enforcement notification • Account suspension	Appendix 2
I.8	**Theft/hack associations**	**HIGH (9) – BLOCK**	• **IMMEDIATE TRANSACTION BLOCK** • SMR filing • Victim notification (if appropriate) • Cooperation with law enforcement	Appendix 2
I.9	**Recent mixing service use (<7 days)**	**HIGH (7)**	• Enhanced verification • Purpose inquiry • Consider blocking • SMR if suspicious	Appendix 2
I.10	**High-risk jurisdiction wallet (North Korea, Iran wallets)**	**HIGH (9) – BLOCK**	• **IMMEDIATE TRANSACTION BLOCK** • Sanctions compliance check • DFAT notification • Account suspension	Appendix 2
I.11	**Privacy coin conversions (regular pattern)**	**MEDIUM-HIGH (6)**	• Enhanced monitoring • Purpose verification • Consider restrictions • SMR if evasion suspected	Appendix 2

J. TRAVEL RULE SPECIFIC RED FLAGS (Effective 31 March 2026)

Item #	Travel Rule Issue	Risk Score	Action Required	Program Reference
J.1	**Incomplete originator information (VASP-to-VASP, ANY amount)**	**HIGH (7)**	• Transaction hold • Request complete information • 3 attempts over 24hrs • Cancel if not resolved	Section 25.5
J.2	**Non-responsive counterparty VASP**	**MEDIUM-HIGH (6)**	• Document 3+ failed attempts • Escalate to AML/CTF CO • Consider blocking future transactions • Remove from approved VASP list if pattern	Section 25.5
J.3	**Geographic inconsistencies (Australian customer → high-risk VASP)**	**HIGH (7)**	• Enhanced verification • Purpose of transfer inquiry • Consider blocking • SMR if suspicious	Appendix 2
J.4	**Counterparty VASP not on approved list**	**MEDIUM-HIGH (6)**	• **INITIATE VASP CDD (Appendix 4)** • Transaction hold pending approval • Reject if VASP fails due diligence	Section 25.4
J.5	**Customer unable to identify beneficiary VASP**	**MEDIUM (4)**	• Educate customer • Verify wallet address ownership • Enhanced monitoring	Section 25.5
J.6	**Inconsistent Travel Rule data vs. known customer data**	**HIGH (7)**	• Investigation mandatory • Transaction hold • Verify with customer • SMR if identity fraud suspected	Section 25.5

Item #	Travel Rule Issue	Risk Score	Action Required	Program Reference
J.7	**Frequent high-value self-hosted transfers (≥$10k)**	**MEDIUM-HIGH (6)**	• Enhanced due diligence • Wallet ownership demonstration • Source of funds verification • AUSTRAC reporting	Section 25.2 (Scenario 2)
J.8	**VASP counterparty sanctions hit**	**HIGH (9) - BLOCK**	• **IMMEDIATE TRANSACTION BLOCK** • Remove from approved VASP list • DFAT/AUSTRAC notification • SMR filing	Section 25.7
J.9	**Travel Rule data quality issues (systematic errors)**	**MEDIUM (4)**	• Technical investigation • Vendor (Sumsub/Notabene) escalation • Manual review of affected transactions	Section 25.4
J.10	**Unusual VASP-to-VASP patterns (high frequency)**	**MEDIUM (4)**	• Profile review • Purpose verification • Enhanced monitoring	Appendix 2

K. CORPORATE/TRUST/ENTITY SPECIFIC RED FLAGS

Item #	Red Flag Description	Risk Score	Action Required	Program Reference
K.1	**Complex ownership structure (>3 layers, no commercial rationale)**	**HIGH (7)**	• Enhanced beneficial ownership verification • Ultimate individual owners required • AML/CTF CO approval • Consider rejection	Sections 35, 43
K.2	**Offshore entities in secrecy jurisdictions (BVI, Cayman, Panama, etc.)**	**MEDIUM-HIGH (6)**	• Enhanced CDD • Source of wealth documentation • Additional certified documents • Ongoing enhanced monitoring	Section 35

Item #	Red Flag Description	Risk Score	Action Required	Program Reference
K.3	**Beneficial ownership unclear (cannot identify ultimate individuals)**	**HIGH (8)**	• Disclosure certificate required • Enhanced investigation • Reject if ownership cannot be established • SMR if evasion suspected	Sections 43, 47
K.4	**Nominee directors/shareholders**	**MEDIUM-HIGH (6)**	• Identify ultimate beneficial owners • Verify commercial arrangement • Enhanced monitoring	Section 43
K.5	**Recently incorporated shell company (<12 months, minimal activity)**	**HIGH (7)**	• Enhanced due diligence • Business plan verification • Source of funds for crypto purchases • Consider rejection	Section 35
K.6	**Cash-intensive business**	**MEDIUM-HIGH (6)**	• Enhanced source of funds verification • Business activity verification • Ongoing enhanced monitoring • Structuring awareness	Appendix 2
K.7	**No clear business purpose (company/trust exists with no obvious activity)**	**HIGH (8)**	• Purpose investigation • Commercial rationale required • Consider rejection • SMR if suspicious	Appendix 2
K.8	**Frequent ownership changes (directors, shareholders, beneficial owners)**	**MEDIUM-HIGH (6)**	• Investigation of each change • Updated KYC for new parties • Pattern analysis • Enhanced monitoring	Section 15.6
K.9	**Inconsistent corporate documents**	**HIGH (7)**	• Document verification • Legal review if necessary • Certified copies required • Consider rejection	Sections 35, 46
K.10	**Reluctance to provide corporate documents (trust deed, shareholder register)**	**HIGH (7)**	• Mandatory documentation • Enhanced CDD • Reject if refused • SMR if suspicious	Sections 35-36

Item #	Red Flag Description	Risk Score	Action Required	Program Reference
K.11	**SMSF irregularities (no ATO registration, unusual trustees, pension phase issues)**	**MEDIUM-HIGH (6)**	• ATO registration verification • Trustee identity checks • SMSF structure review • Consider rejection if non-compliant	Section 36
K.12	**Related party transactions (no commercial justification)**	**MEDIUM (4)**	• Purpose verification • Commercial rationale documentation • Enhanced monitoring	Appendix 2
K.13	**Dormant company suddenly active**	**MEDIUM-HIGH (6)**	• Investigation of activity resumption • New director/shareholder verification • Source of funds • Enhanced monitoring	Appendix 2
K.14	**Business address is virtual office/mail forwarding**	**MEDIUM-HIGH (6)**	• Verify actual operations location • Principal place of business documentation • Enhanced CDD • Consider shell company risk	Appendix 2
K.15	**Industry inconsistent with crypto use (traditional business, no tech rationale)**	**MEDIUM (4)**	• Purpose verification • Business case documentation • Enhanced monitoring	Appendix 2

L. SOURCE OF FUNDS RED FLAGS

Item #	Red Flag Description	Risk Score	Action Required	Program Reference
L.1	**Cannot verify source of funds**	**HIGH (8)**	• Enhanced documentation required • Bank statements, tax returns, payslips	Section 30

Item #	Red Flag Description	Risk Score	Action Required	Program Reference
			• Reject if unverifiable • SMR if suspicious	
L.2	**Inconsistent source of wealth (declared income/assets vs. transaction volume)**	**MEDIUM-HIGH (6)**	• Source of wealth verification • Asset ownership documentation • Enhanced monitoring • SMR if criminal proceeds suspected	Appendix 2
L.3	**Non-employment income (gambling, gifts, inheritance - minimal documentation)**	**MEDIUM (4)**	• Additional documentation required • Verify legitimacy • Enhanced monitoring	Appendix 2
L.4	**Offshore funds access (unexplained)**	**MEDIUM-HIGH (6)**	• Offshore account documentation • Tax compliance verification • Purpose of offshore structure • Enhanced monitoring	Appendix 2
L.5	**Recent large inheritance/windfall (minimal documentation)**	**MEDIUM (4)**	• Inheritance documentation • Deceased estate papers • Bank statements showing transfer • Enhanced verification	Appendix 2
L.6	**Self-employed with complex income (difficult to verify)**	**MEDIUM (4)**	• Tax returns (2+ years) • Business financials • Bank statements • Enhanced monitoring	Appendix 2

M. ADVERSE EVENT TRIGGERS (Immediate Risk Assessment Review Required)

Category	Trigger Event	Action Required
Regulatory	• AUSTRAC enforcement action/warning • Regulatory examination findings • Changes to AML/CTF Act or Rules	• Immediate Program review • Board notification within 24hrs • Risk assessment update

Category	Trigger Event	Action Required
	• New FATF recommendations • Sanctions list updates affecting customers	• Control enhancement if needed • Document lessons learned
Operational	• Significant compliance breach (missed SMR, failed Travel Rule) • Fraud incident (>$10k loss) • Data breach/cybersecurity incident • Employee misconduct (AML/CTF related) • Systematic control failure	• Incident investigation • Root cause analysis • Corrective action plan • Independent review if severe • Staff retraining if needed
Business	• New cryptocurrency assets • New geographic markets • New payment methods • Customer base growth >50% in 3 months • Customer risk profile shift • New products/services	• Risk assessment for change • Board approval • Enhanced monitoring for new activity • Staff training on new risks • Technology/process updates
External	• Major ML/TF incident in VASP sector • New ML/TF typology (AUSTRAC alert) • Sanctions developments • Adverse media coverage (CoinPort) • VASP counterparty enforcement action	• Threat assessment • Control effectiveness review • Enhanced monitoring if relevant • Customer communication if needed • Risk mitigation strategy

N. KEY RISK INDICATORS (KRIs) – MONTHLY DASHBOARD

KRI	Target	Red Flag Threshold	Responsible
SMR submission rate	>0 when suspicious activity detected	Failure to submit within timeframe	AML/CTF CO
TTR submission rate (>$10k)	100% within 10 business days	<95% compliance	AML/CTF CO
Travel Rule message success rate	>95% (from 31 March 2026)	<90%	AML/CTF CO

KRI	Target	Red Flag Threshold	Responsible
False positive rate (transaction monitoring)	<30%	>50%	AML/CTF CO
Customer KYC refresh completion	>95% on schedule	<90%	Operations
Staff training completion	100% annually	<100%	AML/CTF CO
Sanctions screening coverage	100%	<100%	Technology
AMLBot alert response time	<24 hours	>48 hours	AML/CTF CO
VASP counterparty approval time	<3 business days	>5 business days	AML/CTF CO
Independent review findings	Zero critical	Any critical findings	Board

---

DOCUMENT CONTROL

Version	**Date**	**Author**	**Changes**
1.0	[Old Date]	[Name]	Original Coin Harbour matrix
2.0	[Old Date]	[Name]	Updated country lists
3.0	**5 January 2026**	**Nicanor Nuqui**	**Complete overhaul for 2026 reforms:** • Company name: Coin Harbour → CoinPort • Part A/Part B → Unified structure • Added Travel Rule (Section 25) • Added Proliferation Financing (Section 14A) • Added AMLBot blockchain analytics • Added VASP counterparty CDD • Updated all section references • Added 55+ fraud screening

Version	**Date**	**Author**	**Changes**
			• Risk-based scoring (1-9 scale) • Comprehensive red flag appendix integration

Next Review: February 2026 (post-implementation), then April 2026 (quarterly)
Owner: AML/CTF Compliance Officer (Nicanor Nuqui)
Approved By: Board of Directors, 5 January 2026

END OF RISK ASSESSMENT MATRIX

CoinPort Pty Ltd | AUSTRAC Registration: 100633359 | Version 3.0 - 5 January 2026