



SAR Submission Framework

Version 1.1 | Effective 1 January 2026

Introduction

This framework provides Institute standards for SAR (Suspicious Activity Report) submission in the context of cryptoasset compliance. It covers legal obligations under POCA 2002, threshold standards, timing requirements, and crypto-specific considerations.

Authority: This framework is the authoritative reference for TCCS examination content on Domain 4 (Regulatory Compliance & Reporting). All examination marking criteria and model answers are derived from this framework.

1. Legal Obligations Under POCA 2002

Key Sections:

Section 330: Failure to disclose (regulated sector) - applies to all compliance officers, MLROs, designated persons

Section 331: Failure to disclose (nominated officers/MLROs) - higher standard, no 'reasonable excuse' defense

Section 332: Failure to disclose (all persons) - applies to any person who knows or suspects money laundering through business activities

Section 333A: Tipping off - criminal offense to disclose SAR filing or investigation to subject

Section 335: Consent SARs (DAML - Defence Against Money Laundering) - required when transaction would otherwise constitute money laundering offense

2. Knowledge vs Suspicion: The Threshold Standard

INSTITUTE POSITION: The Suspicion Threshold

The Institute's position is that the legal threshold is knowledge OR suspicion, not proof. Suspicion is a lower standard than belief and significantly lower than certainty. Waiting for evidence or proof before filing violates POCA 2002.

Minimum Acceptable Standard: If red flags exist that would cause a reasonable person in the same position to suspect money laundering, a SAR must be filed. Absence of definitive proof is irrelevant.

Common Misapplication (Exam Risk): Candidates state 'we need more evidence before filing' or 'suspicion alone isn't enough'. This is legally incorrect and will lose marks.

Decision Flowchart: Knowledge vs Suspicion

Question	Decision
Do you KNOW money laundering is occurring?	→ FILE SAR IMMEDIATELY
Do red flags exist that would cause a reasonable person to SUSPECT money laundering?	→ FILE SAR
Are you uncertain whether suspicion threshold is met?	→ Consult MLRO, document consultation, file if MLRO agrees
Do you lack definitive proof of money laundering?	→ IRRELEVANT - file if suspicion exists
Would waiting for more evidence delay filing?	→ FILE NOW - waiting is non-compliant

Key Principle: When in doubt, file. Defensive SAR filing is lawful and protected. False negatives (not filing when you should) create criminal liability. False positives (filing when unnecessary) do not.

3. Timing Requirements

INSTITUTE POSITION: SAR Filing Timing

The Institute's position is that SARs must be filed as soon as practicable after suspicion arises. 'As soon as practicable' means within working days, not weeks. Delays create criminal liability under POCA s330-332.

Practical Guidance:

- Simple cases: File within 1-2 working days
- Complex cases requiring MLRO consultation: File within 5 working days
- Ongoing transactions requiring consent: File consent SAR immediately

When This Becomes Unsuitable: Filing weeks after suspicion arises is non-compliant. Document any delays and rationale. Routine delays (e.g., 'we always wait for month-end') are indefensible.

4. Escalation Decision Logic

When to file immediately vs consult MLRO first:

Scenario	Action
Clear knowledge of money laundering (e.g., customer admits criminal source)	File immediately - inform MLRO concurrently
Clear suspicion with multiple red flags	File - may inform MLRO first if time permits
Borderline case - unclear if suspicion threshold met	Consult MLRO - document consultation - file if MLRO agrees
Customer demands immediate transaction (consent SAR scenario)	File consent SAR immediately - consult MLRO concurrently
Ongoing relationship - suspicion emerges during monitoring	File SAR - inform MLRO - review entire relationship

Critical Note: MLRO consultation does not delay filing obligation. If consultation cannot occur within 24-48 hours, file and inform MLRO afterwards.

5. Consent SARs (DAML - Defence Against Money Laundering)

A consent SAR is required when proceeding with a transaction would constitute a money laundering offense (sections 327-329 POCA).

INSTITUTE POSITION: Consent SAR Timing

The Institute's position is that consent SARs must be filed BEFORE proceeding with the transaction. Filing after the fact provides no defense. If consent is refused or 7 working days elapse without response, the transaction must be refused.

Timeline:

- Day 0: File consent SAR
- Day 7: Automatic consent if no NCA response ('notice period')
- NCA may extend moratorium period up to 31 days if investigation ongoing

Common Misapplication (Exam Risk): Candidates proceed with transaction while 'waiting for consent'. This is a substantive money laundering offense (s328 POCA). The transaction must be frozen until consent granted.

Decision Tree: When to File Consent SAR

Question	Decision
Does transaction involve suspected criminal property?	→ Consider consent SAR
Would proceeding facilitate acquisition, use, or possession of criminal property?	→ File consent SAR BEFORE proceeding
Is customer demanding immediate transaction?	→ File consent SAR immediately - do NOT proceed without consent
Can you refuse transaction without 'tipping off'?	→ Refuse using neutral reason (e.g., 'unable to process at this time')
Is transaction already complete when suspicion arises?	→ File standard SAR (not consent SAR) - no defense available post-facto

Key Principle: If in doubt whether consent SAR is required, file it. Over-caution is defensible. Under-caution creates criminal liability.

6. Crypto-Specific SAR Considerations

SAR narratives involving cryptoassets must include:

1. Wallet addresses (originator and beneficiary)
2. Transaction IDs (txids) for relevant transactions
3. Blockchain network (Bitcoin, Ethereum, etc.)
4. Amounts and timestamps (UTC preferred)
5. Source/destination exchange or service (if known)
6. Red flags observed (mixer use, peel chains, high-risk jurisdictions)
7. Blockchain forensics evidence (e.g., Chainalysis/Elliptic risk scores if available)

INSTITUTE POSITION: Blockchain Evidence in SARs

The Institute's position is that wallet addresses and transaction IDs are essential, not optional. SARs lacking this information hinder NCA investigations and may be rejected as incomplete.

Minimum Acceptable Standard: Include all on-chain data available at time of filing. If customer provides incomplete information, state this explicitly in SAR narrative.

7. Record Retention Requirements

Minimum retention: 5 years from date of SAR filing (MLRs 2017 Regulation 40)

Records to retain:

- SAR submission receipt/reference number
- SAR narrative and supporting documentation
- Internal decision logs (why SAR was filed)
- MLRO consultation records (if applicable)
- Consent SAR: NCA response or evidence of 7-day notice period expiry
- Blockchain evidence (wallet addresses, txids, forensic reports)

TrustCrypto Institute

SAR Submission Framework v1.1

Effective: 1 January 2026

(This framework is the authoritative reference for TCCS examination Domain 4)