

# ACAMS - CCAS - Useful Certified Cryptoasset Anti-Financial Crime Specialist Examination Test Simulator

## CCAS Certified Cryptoasset Anti-Financial Crime Specialist Certification Questions and Answers Latest Version (2024/2025) Already Passed

What is the main purpose of anti-financial crime measures in the cryptoasset industry?

- a) To prevent market volatility
- b) To prevent illicit activities like money laundering and fraud
- ✓✓c) To ensure compliance with legal and regulatory standards
- d) To increase market liquidity

How do financial institutions typically identify suspicious transactions in the cryptoasset market?

- a) By tracking high transaction fees
- ✓✓b) By analyzing transaction patterns and connections to high-risk jurisdictions
- c) By monitoring employee activities
- d) By measuring the value of assets held

What is the role of Know Your Customer (KYC) in preventing financial crime in the cryptoasset industry?

1

BONUS!!! Download part of Test4Engine CCAS dumps for free: <https://drive.google.com/open?id=18vWv9JlIU8fjCsMMidyLXoe9kYz3Qf>

The Certified Cryptoasset Anti-Financial Crime Specialist Examination (CCAS) certification exam is one of the hottest and most industrial-recognized credentials that has been inspiring beginners and experienced professionals since its beginning. With the Certified Cryptoasset Anti-Financial Crime Specialist Examination (CCAS) certification exam successful candidates can gain a range of benefits which include career advancement, higher earning potential, industrial recognition of skills and job security, and more career personal and professional growth.

## ACAMS CCAS Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none"><li>• Cryptoasset and Blockchain: This domain targets Blockchain Analysts and Crypto Risk Managers. It focuses on understanding cryptoasset technologies, blockchain fundamentals, and their operational characteristics. Candidates learn about cryptoasset transaction flows, wallets, exchanges, smart contracts, and the challenges these present to financial crime prevention.</li></ul>

Topic 2	<ul style="list-style-type: none"> <li>• AML Foundations for Cryptoasset and Blockchain: This section of the exam measures skills of Anti-Money Laundering (AML) Officers and Crypto Compliance Specialists. It covers foundational knowledge of AML principles tailored to the cryptoasset and blockchain environment, introducing the regulatory landscape, typologies of financial crime, and the evolving risks associated with cryptoassets.</li> </ul>
Topic 3	<ul style="list-style-type: none"> <li>• Risk Management Programs for Cryptoasset and Blockchain: This section measures expertise of Compliance Managers and Risk Officers in developing and implementing risk management frameworks specifically for the crypto sector. It includes procedures for assessing crypto-related financial crime risks, designing controls, monitoring compliance, and adapting to emerging threats within the cryptoasset ecosystem.</li> </ul>

>> CCAS Test Simulator <<

## 2025 ACAMS CCAS: Certified Cryptoasset Anti-Financial Crime Specialist Examination –The Best Test Simulator

Test4Engine is a wonderful study platform that can transform your effective diligence in to your best rewards. By years of diligent work, our experts have collected the frequent-tested knowledge into our CCAS exam materials for your reference. So our practice materials are triumph of their endeavor. By resorting to our CCAS Exam Materials, we can absolutely reap more than you have imagined before. We have clear data collected from customers who chose our CCAS practice materials, and the passing rate is 98-100 percent.

### ACAMS Certified Cryptoasset Anti-Financial Crime Specialist Examination Sample Questions (Q26-Q31):

#### NEW QUESTION # 26

The "indirect exposure" concept in blockchain analytics means:

- A. Funds held in a cold wallet.
- B. Funds sent to OTC brokers.
- C. Funds directly linked to illicit addresses.
- **D. Funds linked via intermediary addresses.**

**Answer: D**

Explanation:

Indirect exposure refers to connections through one or more hops to illicit addresses. This requires robust transaction chain analysis to detect hidden ML/TF risk.

#### NEW QUESTION # 27

Which activity is most commonly associated with mixing and tumbling as a method of laundering cryptoassets?

- **A. Presence of unknown or disguised source of funds**
- B. Frequent transactions to high-risk jurisdictions via different virtual asset service providers
- C. Use of IP address concealing software
- D. Rapid purchase and sale of different cryptocurrencies

**Answer: A**

Explanation:

Mixing and tumbling services are used to obscure the origin of funds by blending multiple transactions, resulting in unknown or disguised sources of funds. This is a classic money laundering technique.

Rapid trades (B), IP address obfuscation (C), and transactions to high-risk jurisdictions (D) are separate or related risks but not direct indicators of mixing/tumbling.

### NEW QUESTION # 28

How should an investigator use transaction history to determine whether cryptoassets were previously involved in money laundering?

- A. Assess other assets held by the cryptoasset owner.
- **B. Assess the cryptoasset addresses' receiving exposure to illicit activity.**
- C. Assess the jurisdiction where the transactions took place.
- D. Assess the identity of the cryptoasset owner.

**Answer: B**

Explanation:

In the context of AML/CFT frameworks for cryptoassets, the investigation of transaction histories involves blockchain analysis tools to trace the flow of funds to and from crypto addresses. Specifically, it is essential to assess whether the addresses involved have had prior exposure to illicit activities such as known darknet marketplaces, ransomware payments, or sanctioned entities. This form of "address screening" helps identify potentially tainted cryptoassets.

The DFSA AML Module and associated guidance emphasize that transaction monitoring for cryptoassets requires analyzing the provenance of funds, not just ownership. While identifying the owner is part of customer due diligence (CDD), the transactional exposure itself reveals laundering risks embedded in the chain of transfers.

Extract from DFSA AML Module and COB Module on Crypto Business Rules:

"Transaction monitoring systems must include blockchain analysis to detect suspicious activity related to crypto tokens, including tracing transactions against known illicit sources."

"Enhanced due diligence (EDD) is required when a cryptoasset transaction involves addresses or wallets with a history of illicit activity."

"Risk-based approaches must integrate forensic review of transaction histories to assess financial crime risks in crypto asset transfers" 【AML/VER25/05-24: Sections 6.3, 7.3, 13.3; COB/VER45/05-24: Sections 6.13, 15】.

Therefore, assessing the receiving exposure of cryptoasset addresses to illicit activity (Option B) is the most direct and effective method to detect laundering.

### NEW QUESTION # 29

What three classifications of assets does the Markets in Crypto-Assets Regulation (commonly known as MICA) apply to? (Select Three.)

- A. Privacy coins
- **B. Asset-referenced tokens**
- **C. Cryptoassets**
- **D. Electronic money tokens**
- E. Meme coins

**Answer: B,C,D**

Explanation:

The EU's Markets in Crypto-Assets Regulation (MICA) applies specifically to:

Electronic Money Tokens (B): Tokens that fulfill the definition of electronic money under the E-Money Directive.

Cryptoassets (D): Broad category including digital representations of value that are not covered by existing financial services legislation.

Asset-Referenced Tokens (E): Tokens that purport to maintain a stable value by referencing one or several assets.

Meme coins (A) and privacy coins (C) are not separately classified under MICA but may fall under broader cryptoasset categories subject to other regulations.

### NEW QUESTION # 30

In cryptoasset compliance, "integration" refers to:

- A. Transferring crypto between wallets.
- B. Staking assets to earn rewards.
- C. Mixing crypto to hide origins.
- **D. Converting illicit crypto into fiat or legitimate assets.**

**Answer: D**

Integration is the final stage of money laundering, where illicit funds re-enter the economy appearing legitimate - e.g., converting crypto into fiat via exchanges or buying assets.

.....

**Test CCAS Simulator Free:** [https://www.test4engine.com/CCAS\\_exam-latest-braindumps.html](https://www.test4engine.com/CCAS_exam-latest-braindumps.html)

- DOWNLOAD the newest Test4Engine CCAS PDF dumps from Cloud Storage for free: <https://drive.google.com/open?id=18vWv9JlllU8frjCsMMidyLXoe9kYz3Qf>