DirectCertify

Unlock Your Potential, Certify Your Success

Acams

CCAS Exam

Certified Cryptoasset Anti-Financial Crime Specialist Examination

Exam Latest Version: 6.0

DEMO Version

Full Version Features:

• 90 Days Free Updates

• 30 Days Money Back Guarantee

• Instant Download Once Purchased

• 24 Hours Live Chat Support

Full version is available at link below with affordable price.

https://www.directcertify.com/acams/ccas

Question 1. (Single Select)

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

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

Correct Answer: C

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"0 AML/VER25/05-2 COB/VER45/05-24: Sections 6.13, 150 .

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

Question 2. (Multi Select)

Which features are used by anonymity-enhanced cryptoassets to reduce transparency of transactions and identities? (Select Two.)

A: Proof-of-stake mining
B: Automatic mixing
C: Secure hashing algorithm 256
D: Cryptographic enhancements
E: MetaMask wallet

Correct Answer: B, D

Explanation:

Anonymity-enhanced cryptoassets employ specific technical features to obfuscate the details of transactions and the identities of users to reduce traceability and increase privacy. These include:

Automatic mixing (B): This refers to mechanisms such as coin mixers or tumblers that combine multiple transactions from different users into one batch and redistribute them, breaking the direct transaction link and obscuring the audit trail.

Cryptographic enhancements (D): Techniques such as zero-knowledge proofs, ring signatures, stealth addresses, and confidential transactions are cryptographic protocols that conceal sender, receiver, and transaction amount information, making the blockchain ledger less transparent.

Other options explained:

Proof-of-stake mining (A) is a consensus mechanism and not related to anonymity features.

Secure hashing algorithm 256 (C) is a cryptographic hash function standard but does not directly enhance anonymity.

MetaMask wallet (E) is a non-custodial wallet used mainly for Ethereum and tokens but is not an anonymity tool.

Reference from official crypto AML guidance and typology papers:

DFSA AML Module and thematic reviews highlight these anonymity techniques as high-risk indicators requiring enhanced due diligence (EDD).

UAE typology papers and FATF virtual asset guidance emphasize the risk posed by anonymity-enhanced cryptoassets using automatic mixing and cryptographic enhancements to circumvent AML controls0 AML/VER25/05-24: Sections 6.4, 7.3; 31.92._TFS_Typology_Paper_Eng__4.pdf0 .

Question 3. (Single Select)

Which is the first action a virtual asset service provider (VASP) should take when it finds out that its customers are engaging in virtual asset (VA) transfers related to unhosted wallets and peer-to-peer (P2P) transactions?

A: Allow VA transfers related P2P or unhosted wallets below 1,000 USD or the equivalent amount in local currency, or per defined thresholds in local regulations.
B: Freeze accounts with records of transactions related to P2P transactions or unhosted wallets.
C: Collect and assess the data on transactions related to P2P or unhosted wallets to determine if it is within its risk appetite.
D: Enhance existing risk-based control framework to account for specific risks posed by transactions related to P2P or unhosted wallets.

Correct Answer: C

Explanation:

Upon identifying customer engagement with unhosted wallets or P2P transfers, the first step a VASP should take is to collect and assess data on such transactions. This assessment helps determine if these activities fall within the firm's risk appetite and what enhanced controls or actions may be needed.

Immediate account freezing (B) is not the first step without assessment; neither is allowing transfers (A) without risk consideration. Enhancing risk frameworks (D) is important but follows from an initial data-driven risk assessment.

Relevant guidance:

FATF Recommendations and DFSA AML Module require VASPs to maintain a risk-based approach that begins with data collection and risk assessment on unhosted wallet transactions.

The DFSA's 2023 Dear MLRO letters and thematic reviews stress proportionality and evidence-based responses rather than immediate punitive measures.

Enhanced due diligence (EDD) and risk mitigation measures, including potentially freezing accounts, come after assessment of the risk level0 AML/VER25/05 20230406Dear_MLRO_Letter_re_IEMS.pdf0 .

Hence, C is the appropriate first action.

Question 4. (Single Select)

In a blockchain 51% attack, what does 51% refer to?

A: Governance tokens
B: Wallets
C: Computational power required for mining
D: Exchanges

Correct Answer: C

Explanation:

A 51% attack refers to a situation where a single miner or group controls more than 50% of the blockchain network's computational (hashing) power. This majority control allows them to manipulate the blockchain ledger by double-spending or blocking transactions.

This term is widely recognized in blockchain security contexts and is referenced in typology papers on crypto financial crime risks, including those issued by UAE authorities and FATF.

Supporting extracts:

DFSA AML thematic reviews mention the risk of manipulation and double spending in blockchains susceptible to 51% attacks.

Typology reports on cryptoasset risks highlight computational power concentration as a core

vulnerability.

“51% refers to the percentage of total mining power or computational power in the network” is the standard definition across crypto AML/CFT frameworks0 31.92._TFS_Typology_Paper_Eng__4.pdf; AMLCFT_G

Thus, C is correct.

Question 5. (Multi Select)

How does law enforcement use Suspicious Activity Reports (SARs)? (Select Two.)

A: To identify regulatory failings
B: To produce evidence of money laundering that can be used in court
C: To develop intelligence on new targets
D: To confirm or develop information on existing targets

Correct Answer: C, D

Explanation:

Suspicious Activity Reports (SARs) are a critical tool for law enforcement agencies. They are primarily used to develop intelligence on potential new criminal targets and to confirm or expand information about existing investigations. SARs do not serve as direct evidence of money laundering in court but provide leads and context that enable law enforcement to build cases.

The DFSA’s thematic reviews and AML guidance clarify that SARs assist in identifying emerging crime patterns and help intelligence units track suspicious transactions over time. They also allow law enforcement to corroborate data from other sources.

SARs help:

Develop intelligence on new targets (C) by revealing previously unknown suspicious behavior.

Confirm or develop information on existing targets (D) by adding transactional data and context.

Identifying regulatory failings (A) is primarily a supervisory function, and SARs themselves are not evidence for prosecution (B) but intelligence inputs.

Therefore, options C and D are correct.

DirectCertify

Unlock Your Potential, Certify Your Success

Full version is available at link below with affordable price.

https://www.directcertify.com/acams/ccas

30% Discount Coupon Code: LimitedTime2025