KaozhengPro

IT認證考試題庫

專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

Exam : **CCAS**

Title : Acams Certified Cryptoasset Anti-Financial Crime Specialist Examination

Version : DEMO

1.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.
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"【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 C) is the most direct and effective method to detect laundering.

2.A compliance officer at an exchange who is conducting an annual risk assessment identifies an increased volume of transactions to and from unhosted wallets.
Based on Financial Action Task Force guidance, which inherent risk rating would be most appropriate for the compliance officer to assign to such activities?
A. Negligible
B. Low
C. Moderate
D. High
Answer: D
Explanation:
The Financial Action Task Force (FATF) guidance on Virtual Assets and Virtual Asset Service Providers (VASPs) explicitly highlights that transactions involving unhosted wallets (wallets not held or controlled by a regulated entity) pose a high inherent risk for money laundering and terrorist financing. This is because unhosted wallets are more difficult to monitor and control, lack identifiable customer information, and are often exploited for illicit activities.
The DFSA AML Module, aligned with FATF recommendations, mandates that Relevant Persons

incorporate this risk into their business-wide risk assessments. The increased volume of transactions to and from unhosted wallets should therefore be assigned a high inherent risk rating to trigger enhanced controls such as enhanced due diligence (EDD) and transaction monitoring.
Supporting extracts include:
FATF Guidance on Virtual Assets (October 2021) states: "Unhosted wallets or transactions with them represent a high risk of ML/TF due to limited or no access to identifying information."
DFSA AML Module (AML/VER25/05-24) Section 4.1 & 6.1 on Risk-Based Approach: mandates firms to assess and rate risks posed by customers and products, explicitly including virtual assets and unhosted wallets as high risk.
COB Module also requires heightened controls and disclosures when dealing with transactions involving unhosted wallets【AML/VER25/05-24: Sections 4.1, 6.1, COB/VER45/05-24: Sections 6.13, 15.6】.
Thus, option D (High) is the correct risk rating.

3.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
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 controls【AML/VER25/05-24: Sections 6.4, 7.3; 31.92._TFS_Typology_Paper_Eng__4.pdf】.

4.What is indirect exposure in regards to blockchain analytics transaction monitoring?
A. The cryptoassets are absolutely linked to a specific user and identity on the blockchain.
B. The cryptoassets have a connection to risky activity via another crypto address or addresses.
C. The cryptoassets went through a mixing protocol to conceal source of funds.
D. The fiat currency is not immediately linked to a known bank account.
Answer: B
Explanation:
Indirect exposure refers to a situation where cryptoassets are not directly associated with illicit activity but have transactional links through other addresses that are associated with risky or illicit behavior. Blockchain analytics tools detect these indirect links to flagged addresses, allowing firms to assess risk based on network connections rather than direct ownership or activity.
The DFSA AML guidance and international FATF Virtual Assets guidance explain that indirect exposure is a critical concept for transaction monitoring as it broadens the detection scope beyond direct transactions, flagging assets that might be “tainted” through intermediary addresses.
Reference: FATF Guidance on Virtual Assets and VASPs emphasizes monitoring both direct and indirect exposure of wallets to illicit activity.
DFSA AML Module Section 13 on Suspicious Activity Reports requires firms to incorporate indirect exposure assessments in their monitoring systems【AML/VER25/05-24: Sections 4.1, 6.3, 13.3; FATF VA Guidance 2021】.
Therefore, B is the correct definition.

5.Which level of an organization is ultimately responsible for risk oversight?
A. 1st line compliance team
B. 2nd line compliance team
C. Chief risk officer
D. Board of directors
Answer: D
Explanation:
The ultimate responsibility for risk oversight lies with the Board of Directors. Senior management and the board have the fiduciary and governance duty to ensure that an effective risk management framework, including AML/CFT controls and cryptoasset-specific risks, is in place and functioning properly.
The DFSA GEN Module and AML Module explicitly allocate the highest accountability for compliance and risk oversight to the Board of Directors, while first and second lines support implementation and oversight respectively. The Chief Risk Officer (CRO) supports risk management but the board maintains ultimate accountability.
Key extracts:
GEN Module, Chapter 5: “Responsibility for compliance lies with every member of senior management, with ultimate oversight by the Board.”
AML Module Section 1.2 & 4.1: “Senior management and Board must ensure appropriate systems and controls for AML/CFT risk management.”
FATF Recommendation 2 underscores that senior management and boards are accountable for effective AML governance【GEN/VER64/05-24: Chapter 5; AML/VER25/05-24: Sections 1.2, 4.1】.
Thus, D is the correct answer.