DUMPSBOSS.

Certified Cryptoasset Anti-Financial Crime Specialist Examination

ACAMS CCAS

Version Demo

Total Demo Questions: 12

Total Premium Questions: 120

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

A virtual asset service provider is assessing whether to support a new decentralized finance protocol. Which features would increase the protocol's inherent money-laundering risk? (Select Three.)

A. Rapid transfers of value across multiple blockchains.

B. Pooling of customer assets within common liquidity pools.

C. Administrative powers that can be changed without transparent accountability.

D. Independent review of smart-contract code before deployment.

E. Publication of the protocol's smart-contract code for public review.

ANSWER: A B C

Explanation:

Features that permit rapid, opaque movement of value can materially increase inherent risk. Cross-chain transfers can complicate tracing because investigators must follow assets across multiple networks and bridge arrangements. Pooling customer assets can reduce visibility into the ownership and provenance of individual deposits. Governance or administrative functions that can change protocol controls without transparent accountability can also create material abuse and operational-risk concerns.

Independent code review and transparent publication of smart-contract code are risk mitigants rather than inherent risk drivers. The fact that a protocol uses a public blockchain does not, by itself, establish effective customer identification or transaction-monitoring controls.

QUESTION NO: 2

Which key type of information allows financial intelligence units to combat the risk of anonymity in virtual currencies?

A. The data referring to the timing of the transaction

B. The data reconciling the transaction and the identity of the receiver

C. The data connecting the transaction information to the virtual address

D. The data associating the virtual address to the identity of the owner

ANSWER: D

Explanation:

The data associating the virtual address to the identity of the owner is the key information because it converts a blockchain identifier from a pseudonymous technical reference into actionable financial intelligence about a real person or legal entity. Public blockchain records can reveal transfers, balances, transaction patterns, counterparties, and movement through clusters of addresses, but these details alone ordinarily do not establish who controls an address. Attribution data obtained through customer due diligence, virtual-asset service-provider records, lawful requests, and intelligence sharing enables a financial intelligence unit to connect suspicious on-chain activity to a subject, assess that subject's risk, identify related assets or transactions, and disseminate usable intelligence to competent authorities. This identity-to-address association is therefore central to mitigating the anonymity and pseudonymity risks presented by virtual assets. FATF's virtual-assets standards emphasize the importance of originator and beneficiary information, customer due diligence, recordkeeping, and the ability to make relevant information available to competent authorities. See the FATF Guidance for a Risk-Based Approach to Virtual Assets and VASPs and the FATF virtual-asset red-flag indicators report.

QUESTION NO: 3

A VASP uses machine learning to prioritise transaction-monitoring alerts. Which controls are necessary to manage the model's financial-crime compliance risk? (Select Three.)

A. Independent validation of model performance and limitations.

B. Ongoing monitoring for performance deterioration and emerging typologies.

C. Human review and documented escalation for material alerts and decisions.

D. Removal of manual review to ensure that alert decisions are fully automated.

E. Assumption that historical training data guarantees continued model accuracy.

F. Restriction of model documentation from compliance oversight personnel.

ANSWER: A B C

Explanation:

Independent validation helps confirm that the model performs as intended and remains appropriate for the risks it is designed to identify. Ongoing monitoring for performance deterioration or changes in customer and transaction behaviour is necessary because a model can become less effective as typologies evolve. Human review and documented escalation procedures are also essential for material alerts and decisions, particularly where the outcome may affect customer treatment or suspicious-activity reporting.

Eliminating manual review is not an appropriate control because accountability and professional judgment remain necessary. A model should not be assumed accurate merely because it was trained on historical alerts, and withholding model documentation from compliance oversight prevents effective governance and challenge.

QUESTION NO: 4

Which key differences between the Bitcoin and Ethereum blockchains must investigators consider when investigating flows of funds on each respective chain? (Select Two.)

A. Transaction cost

B. Variety of applications, assets, and networks

C. Address length

D. Ledger model

ANSWER: B D

Explanation:

Variety of applications, assets, and networks is a material investigative distinction because Ethereum fund flows can involve the native ETH asset alongside fungible tokens, non-fungible tokens, smart contracts, decentralized exchanges, lending protocols, bridges, and other decentralized applications. An investigator must therefore identify not only transfers between addresses, but also the asset being moved, the contract interaction creating the movement, and whether value is entering or leaving another blockchain environment. This broader ecosystem can create multi-step and multi-asset transaction paths that require contract- and token-aware tracing.

Ledger model is equally important because Bitcoin generally records value through the unspent transaction output (UTXO) model: transactions consume prior outputs and create new outputs. Fund-flow analysis consequently focuses on transaction inputs, outputs, change addresses, and UTXO linkages. Ethereum instead uses an account-based model, in which transactions alter account balances and may execute smart-contract code. Investigators must interpret sender, recipient, internal value movements, token-transfer events, and contract state interactions in that different accounting structure. These foundational differences directly affect how attribution, transaction histories, and movement of value are reconstructed. See Bitcoin Developer Guide: Transactions and Ethereum.org: Accounts.

QUESTION NO: 5

Which is an accurate description of a Decentralized Autonomous Organization (DAO)?

A. DAOs are decentralized blockchain organizations that require managerial activity by humans.

B. DAOs are organizational structures through which how a protocol will operate is determined by a group of actors.

C. DAOs are cryptocurrency funds in which the board of directors submit their votes using blockchain technology.

D. DAOs are decentralized blockchain technologies that use traditional contracts instead of smart contracts.

ANSWER: B

Explanation:

DAOs are organizational structures through which how a protocol will operate is determined by a group of actors. A DAO establishes rules for collective coordination and governance, commonly using blockchain-based smart contracts and a voting process through which eligible participants, often governance-token holders, can propose and decide on actions. This model enables a protocol or treasury to be governed according to transparent, pre-established procedures rather than through conventional centralized management. The degree of decentralization and the precise voting rights can vary by DAO, but the essential characteristic is that operational or governance decisions are made collectively by a defined community of participants. Smart contracts may automate execution of approved decisions, such as allocating treasury assets or modifying protocol parameters, while participants retain responsibility for deliberation and voting. This description aligns with the Financial Action Task Force's discussion of decentralized applications and arrangements, which recognizes that governance can be exercised by holders of governance tokens or other participants. See the FATF targeted update on virtual assets and VASPs and the Ethereum DAO overview.

QUESTION NO: 6

A beneficiary virtual asset service provider (VASP) receives a transfer without the required originator information. The transfer is otherwise technically valid and the beneficiary is an existing customer. What is the most appropriate action?

A. Credit the transfer because the beneficiary is already subject to CDD.

B. Apply risk-based procedures to determine whether to execute, reject, or suspend the transfer and seek the missing information.

C. Return the transfer automatically because all missing information indicates money laundering.

D. Request the missing information directly from the beneficiary customer before reviewing the originating VASP.

ANSWER: B

Explanation:

The beneficiary VASP should apply documented, risk-based procedures for transfers that arrive with missing required information. Those procedures should determine when to execute, reject, or suspend a transfer and when to seek the missing information from the originating VASP. A technically valid blockchain transfer does not remove the VASP's obligation to manage Travel Rule and AML/CFT risk. Automatically crediting the transfer without review would undermine those controls, while automatically rejecting every incomplete transfer would not reflect the required risk-based approach.

QUESTION NO: 7

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:

Automatic mixing and cryptographic enhancements are features that can reduce the transparency of cryptoasset transactions and users' identities. Automatic mixing, whether integrated into an asset's design or performed through a mixing service, pools or coordinates funds in ways intended to weaken the on-chain link between a source address and a destination address. This makes following the transaction trail more difficult and can complicate blockchain analytics.

Cryptographic enhancements describe privacy-preserving mechanisms embedded in certain cryptoassets. Examples include ring signatures, stealth addresses, confidential transactions, and zero-knowledge proofs. Depending on the protocol, these mechanisms can obscure the sender, recipient, transaction amount, or relationship between transaction inputs and outputs. Their use can therefore limit the information visible to the public and affect the ability of financial institutions, virtual asset service providers, and investigators to trace activity using ordinary blockchain data.

FATF identifies anonymity-enhancing technologies and services, including mixers and privacy-enhancing coins, as factors that may increase virtual-asset money-laundering and terrorist-financing risk and require a risk-based response. See FATF's updated guidance for virtual assets and VASPs and FATF virtual-asset red-flag indicators.

QUESTION NO: 8

Which are essential components of an AML program for Customer Due Diligence (CDD)? (Select Three.)

A. Requirement for training of staff responsible for gathering CDD information

B. Requirement to keep all information necessary to maintain a customer's risk profile

C. Requirement to maintain an accurate and complete list of virtual assets exposed to high risk of misuse

D. Procedures to annually review all clients

E. Procedures to ensure that high-risk customers' IP addresses are subject to ongoing monitoring

F. Procedures to address circumstances where the true identity of a customer is questionable

ANSWER: A B F

Explanation:

"Requirement for training of staff responsible for gathering CDD information," "Requirement to keep all information necessary to maintain a customer's risk profile," and "Procedures to address circumstances where the true identity of a customer is questionable" are essential CDD-program components. Effective CDD depends on personnel being able to obtain, assess, document, and escalate customer-identification and beneficial-ownership information consistently. Training supports accurate execution of those procedures and helps staff recognize gaps, inconsistencies, and risk indicators during onboarding and throughout the relationship.

Maintaining information needed for the customer risk profile is equally central because CDD is not a one-time collection exercise. A customer's expected activity, ownership and control details, geographic exposure, products used, and other relevant risk factors must be retained and kept sufficiently current to support ongoing monitoring and risk-based review. Procedures for situations in which a customer's identity is doubtful ensure that the institution can perform appropriate enhanced inquiry, avoid completing verification on unreliable information, and determine whether escalation or a suspicious-activity report is warranted. FATF Recommendation 10 specifically requires customer identification and verification, understanding the relationship's purpose and intended nature, and ongoing due diligence, including scrutiny and updating of customer information. See FATF Recommendations and FinCEN Customer Due Diligence Rule.

QUESTION NO: 9

Which risk category covers threats from ransomware actors demanding payment in cryptoassets?

A. Operational risk

B. Counterparty risk

C. Cyber-enabled financial crime risk

D. Liquidity risk

ANSWER: C

Explanation:

Cyber-enabled financial crime risk is the applicable category because ransomware is a cybercrime in which threat actors use malicious software to deny access to systems or data and demand a payment, frequently in cryptoassets, in exchange for restoration or a decryption key. The cryptoasset element is central to the financial-crime risk: virtual assets can facilitate rapid, cross-border value transfer and may be exploited by criminals seeking to receive, move, or obscure illicit proceeds. A cryptoasset business's anti-financial-crime framework should therefore recognize ransomware exposure in its risk assessment and apply appropriate controls, including blockchain analytics, transaction monitoring, sanctions screening, escalation, and suspicious-activity reporting where required. FATF identifies ransomware as a form of cyber-enabled crime that generates proceeds involving virtual assets and notes that relevant service providers should identify and mitigate associated money-laundering and terrorist-financing risks. The U.S. Treasury's Office of Foreign Assets Control also emphasizes that ransomware payments can create sanctions exposure, especially where a designated person or jurisdiction is involved. See FATF's Virtual Assets Red Flag Indicators and OFAC's Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments.

QUESTION NO: 10

An exchange receives a customer deposit through the Lightning Network. Why may ordinary on-chain transaction tracing provide incomplete information about the payment path?

A. Individual payments may be routed off-chain and not appear as separate Bitcoin blockchain transactions.

B. Lightning payments cannot be associated with any Bitcoin value.

C. Lightning payments permanently delete the underlying Bitcoin transaction history.

D. Lightning payments can only occur between custodial exchange wallets.

ANSWER: A

Explanation:

Lightning Network payments can be routed through off-chain payment channels. The Bitcoin blockchain records channel funding, closing, and certain settlement activity, but it does not ordinarily record every individual payment routed through the network. As a result, an investigator may need to rely on information held by the exchange, payment service provider, customer, or other relevant counterparties in addition to the base-layer blockchain record.

The limitation does not mean that Lightning payments are anonymous by definition or that they cannot be investigated. It means that the available evidence and tracing approach differ from a conventional Bitcoin transfer recorded directly on-chain.

QUESTION NO: 11

Which token type should be considered as carrying the highest risk when assessing the AML risks related to the customer's source of funds?

A. Privacy

B. Stablecoin

C. Platform

D. Security

ANSWER: A

Explanation:

Privacy is the correct answer because privacy-enhancing cryptoassets are specifically designed to limit the visibility of transaction information, which can include wallet addresses, counterparties, transferred amounts, and transaction histories. When a customer's source of funds includes these assets, the institution may be less able to establish a reliable audit trail, identify the origin of the assets, screen relevant counterparties, or corroborate the customer's explanation of how the funds were acquired. This reduced transparency materially increases the risk that illicit proceeds could be introduced into the financial system without effective detection.

A risk-based assessment should therefore treat privacy-enhancing features as a significant risk factor and apply proportionate controls, such as enhanced due diligence, additional source-of-funds evidence, blockchain-analysis capabilities where technically feasible, and escalation where the origin cannot be satisfactorily established. The Financial Action Task Force identifies anonymity-enhanced cryptocurrencies among the characteristics that may create higher money-laundering and terrorist-financing risk and notes that providers should identify and mitigate such risks under a risk-based approach. See the FATF Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers and FATF's targeted update on implementation of virtual-asset standards.

QUESTION NO: 12

Which of the following are red flag indicators specifically related to anonymity? (Select Two.)

A. Use of decentralized or hardware wallets to transport cryptoassets across borders

B. Users utilizing mixing services

C. Use of privacy-orientated email services

D. Use of cryptoassets that are linked to fraudulent schemes

E. Users exhibiting unusual sign-on activity

ANSWER: A B

Explanation:

"Use of decentralized or hardware wallets to transport cryptoassets across borders" is an anonymity-related red flag because these arrangements can enable peer-to-peer custody and movement of value outside a hosted-wallet relationship. This may reduce the availability of reliable customer-identification, counterparty, and transaction-origin information that a regulated cryptoasset service provider would ordinarily use for customer due diligence and transaction monitoring. The cross-border dimension can further complicate tracing and the timely exchange of information among relevant intermediaries and authorities.

"Users utilizing mixing services" is also directly associated with anonymity. Mixers, also called tumblers, are designed to obscure links between blockchain addresses by pooling, splitting, and redistributing cryptoassets. Although public blockchains retain transaction records, mixing can materially hinder attribution and tracing of source and destination addresses, increasing the risk that illicit proceeds can be layered or moved undetected. FATF's virtual-asset red-flag guidance specifically identifies the use of anonymity-enhancing services or tools, including mixing/tumbling services, and recognizes wallet arrangements that can limit identifying information as relevant indicators requiring risk-based review. See FATF, Red Flag Indicators of Money Laundering and Terrorist Financing Involving Virtual Assets and FinCEN's analysis of ransomware trends and mixer use.