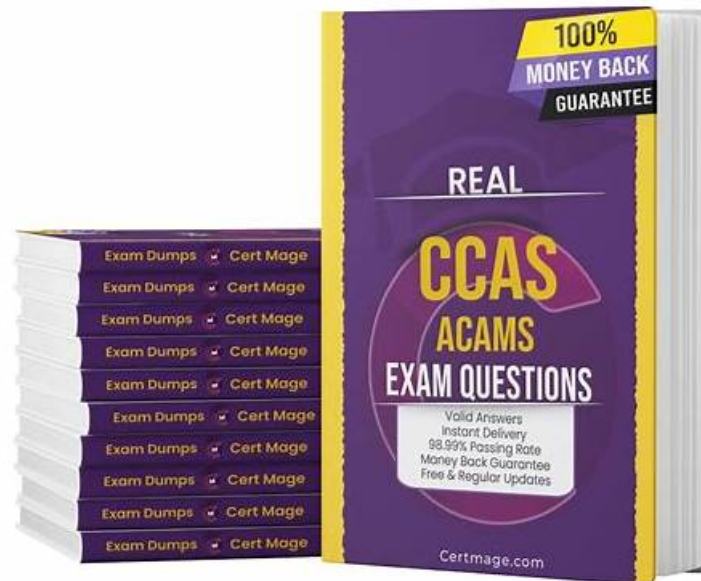


Dumps CCAS Vce - CCAS Valid Exam Blueprint



2026 Latest DumpsKing CCAS PDF Dumps and CCAS Exam Engine Free Share: https://drive.google.com/open?id=1XZDQFRh1795ZrI-W_r5bQLJZSxqeJH_T

Many companies' executives have a job content that purchasing CCAS valid exam collection PDF help their engineers to pass exam and obtain a useful certificate. It is not only improving the qualification of engineers personal but also showing the qualification of companies. If they choose right CCAS valid exam collection PDF they will save a lot of exam cost and dumps fee for companies. Our products will be excellent choice with high passing rate.

Welcome to DumpsKing-the online website for providing you with the latest and valid ACAMS study material. Here you will find the updated study dumps and training pdf for your CCAS certification. Our CCAS practice torrent offers you the realistic and accurate simulations of the real test. The CCAS Questions & answers are so valid and updated with detail explanations which make you easy to understand and master. The aim of our CCAS practice torrent is to help you successfully pass.

>> **Dumps CCAS Vce** <<

Fast Download Dumps CCAS Vce & Pass-Sure CCAS Valid Exam Blueprint & Useful Exam Dumps CCAS Demo

As most of the people tend to use express delivery to save time, our CCAS preparation exam will be sent out within 5-10 minutes after purchasing. As long as you pay at our platform, we will deliver the relevant exam materials to your mailbox within the given time. Our company attaches great importance to overall services, if there is any problem about the delivery of CCAS Exam Materials: Certified Cryptoasset Anti-Financial Crime Specialist Examination, please let us know, a message or an email will be available.

ACAMS CCAS Exam Syllabus Topics:

Topic	Details

Topic 1	<ul style="list-style-type: none"> • 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.
Topic 2	<ul style="list-style-type: none"> • 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.
Topic 3	<ul style="list-style-type: none"> • 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.

ACAMS Certified Cryptoasset Anti-Financial Crime Specialist Examination Sample Questions (Q79-Q84):

NEW QUESTION # 79

Which type of wallet poses the highest AML risk?

- A. Multi-signature wallet
- **B. Unhosted wallet**
- C. Custodial wallet
- D. Exchange hot wallet

Answer: B

Explanation:

Unhosted wallets allow direct user control without third-party oversight, making them harder to monitor and more vulnerable to misuse.

NEW QUESTION # 80

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. Moderate
- B. Negligible
- C. Low
- **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.

NEW QUESTION # 81

Based on Financial Action Task Force guidance, when a cryptoasset exchange carries out an occasional transaction, the exchange is required to conduct CDD when the transaction is above:

- A. USD/EUR 5000.
- B. USD/EUR 1000.
- C. USD/EUR 15000.
- **D. USD/EUR 10000.**

Answer: D

Explanation:

FATF guidance sets the threshold for Customer Due Diligence (CDD) on occasional transactions at USD/EUR 10,000 or equivalent. This means that when a cryptoasset exchange processes a one-off transaction exceeding this amount, it must apply appropriate CDD measures.

This aligns with FATF Recommendation 10 and is adopted by DFSA and FSRA frameworks governing virtual asset service providers, ensuring transactions over this limit are subject to identity verification and risk assessment.

Extracts from AML and COB modules emphasize this threshold as the trigger for CDD on occasional transactions to prevent laundering through high-value single transfers.

NEW QUESTION # 82

Which statement regarding cryptocurrencies, digital assets, and blockchain is correct?

- A. Cryptocurrencies and blockchain are the same and are terms used interchangeably.
- B. Digital assets can only operate on a blockchain.
- C. Cryptocurrencies, blockchain, and digital assets can all be used as a means of payment.
- **D. Cryptocurrencies use encryption techniques operating independently from a central bank.**

Answer: D

Explanation:

Cryptocurrencies are digital currencies secured by cryptography, operating independently from any central bank or government. Blockchain is the underlying distributed ledger technology supporting cryptocurrencies and other digital assets.

Cryptocurrencies and blockchain are not the same (B). Digital assets can exist off-blockchain (C), such as tokenized assets on centralized databases. While cryptocurrencies can be used as payment, blockchain itself is a technology, not a payment method (D).

NEW QUESTION # 83

If a VASP suspects a transaction involves a sanctioned entity, it must:

- A. Report only if over USD 10,000
- B. Wait for law enforcement confirmation
- C. Cancel the customer account immediately without reporting
- **D. File a SAR and freeze assets if required by law**

Answer: D

Explanation:

Sanctions breaches require immediate reporting to competent authorities and freezing of assets where legally mandated.

NEW QUESTION # 84

.....

