

Latest CCAS VCE Torrent & CCAS Pass4sure PDF & CCAS Latest VCE



<http://www.torrentvce.com>

Pass the Actual Test with the Latest Vce Torrent at first attempt

What's more, part of that PassReview CCAS dumps now are free: https://drive.google.com/open?id=1yYnr4gMRhFRiJt3tENtVa_Vk_mc2WYm

I know that you are already determined to make a change, and our CCAS exam materials will spare no effort to help you. After you purchase our CCAS practice engine, I hope you can stick with it. We can promise that you really don't need to spend a long time and you can definitely pass the CCAS Exam. As we have so many customers passed the CCAS study questions, the pass rate is high as 98% to 100%. And this data is tested. With our CCAS learning guide, you won't regret!

ACAMS CCAS Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• 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.
Topic 3	• 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.

>> CCAS Reliable Test Cost <<

Latest CCAS Dumps Files & Exam CCAS Material

Our CCAS practice materials not only apply to students, but also apply to office workers; not only apply to veterans in the workplace, but also apply to newly recruited newcomers. Our CCAS study materials use a very simple and understandable language, to ensure that all people can learn and understand. Our CCAS real test also allows you to avoid the boring of textbook reading, but let you master all the important knowledge in the process of doing exercises. And the high pass rate of our CCAS exam questions is more than 98%. Why not have a try on our CCAS study guide?

ACAMS Certified Cryptoasset Anti-Financial Crime Specialist Examination Sample Questions (Q24-Q29):

NEW QUESTION # 24

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

- A. Cyber-enabled financial crime risk
- B. Counterparty risk
- C. Operational risk
- D. Liquidity risk

Answer: A

Explanation:

Ransomware schemes are categorized as cyber-enabled financial crimes. AML/CFT frameworks require that such risks be assessed and mitigated through blockchain analytics, sanctions screening, and transaction monitoring for known ransomware wallet addresses.

NEW QUESTION # 25

What is the most pertinent item for a cryptoasset money services business to include in a suspicious activity report?

- A. The aggregate total amount of fiat currency used by the subject to purchase cryptocurrency
- B. The names of every owner of the destination wallet address(es) to which the subject sent transactions during the review period
- C. All types of cryptocurrencies purchased by the subject, including aggregate total of each and fiat currency equivalent
- D. The subject's account onboarding information not otherwise included in the counter-party information section

Answer: C

Explanation:

SARs should include detailed transactional information to support investigations, including all types and aggregate amounts of cryptocurrencies purchased, along with fiat currency equivalents. This information provides a clear picture of the subject's activity and financial scale.

Owner names of destination wallets (B) may not be available; onboarding info (D) is supplementary, and fiat aggregate totals (C) alone are insufficient.

FATF and DFSA guidance recommend comprehensive transactional data inclusion in SARs to facilitate law enforcement.

NEW QUESTION # 26

What is a "token burn"?

- A. Sending tokens to a liquidity pool.
- B. Transferring tokens to an OTC desk.
- C. Destroying tokens to reduce supply.
- D. Locking tokens in staking.

Answer: C

Explanation:

A token burn is the deliberate removal of tokens from circulation by sending them to an unspendable address. While sometimes legitimate, burns can also be misused for market manipulation.

NEW QUESTION # 27

In the context of forensic cryptocurrency investigations, which statement best describes how attribution data are collected?

- A. Derived from public and non-public sources.
- B. Obtained automatically from the darknet.
- C. Taken from business-maintained records.
- D. Gathered from a publicly available blockchain.

Answer: A

Explanation:

Attribution data involves linking blockchain addresses to real-world entities, which is derived from a combination of public sources (blockchain explorers, public databases) and non-public sources (law enforcement databases, commercial analytics, exchange records).

Relying solely on blockchain data (C) or darknet sources (D) is insufficient. Business records (A) are part of non-public sources. DFSA and FATF AML guidance underscore the multi-source approach for effective forensic attribution.

NEW QUESTION # 28

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

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

Answer: B

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:

DFSAs 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 frameworks 【31.92. _TFS_Typology_Paper_Eng_4.pdf; AMLCFT_Guidance_for_FIs.pdf】 .

Thus, C is correct.

NEW QUESTION # 29

.....

- BTW, DOWNLOAD part of PassReview CCAS dumps from Cloud Storage: https://drive.google.com/open?id=1yYnr4gMRhFRiJt3tENtVa_Vk_mc2WYm